

明 細 書

管理装置、端末装置及び著作権保護システム

技術分野

- [0001] 本発明は、映画や音楽などの著作物であるコンテンツのデジタル化データを、光ディスク等の大容量記録媒体に記録、あるいは再生するシステムに関し、特に不正装置を使ったコンテンツの記録、あるいは再生による著作権侵害を防止するための技術に関する。

背景技術

- [0002] 近年、マルチメディア関連技術の発展、大容量記録媒体の出現等を背景として、動画、音声等からなるデジタルコンテンツ(以下、コンテンツ)を生成して、光ディスク等の大容量記録媒体に格納して配布する、あるいはネットワークや放送を介して配信するシステムが現れている。

配信されたコンテンツは、コンピュータや再生装置等で読み出されて、再生、あるいはコピーの対象となる。

- [0003] 一般的に、コンテンツの著作権を保護するため、即ちコンテンツの不正再生や不正コピーといった不正利用を防止するために暗号化技術が用いられる。

具体的には、コンテンツをある暗号化鍵を用いて暗号化して光ディスク等の記録媒体に記録して配布する。これに対して、その暗号化鍵に対応する復号鍵を保有する端末のみが、記録媒体から読み出したデータをその復号鍵を用いて復号して、コンテンツの再生等を行うことができる、というものである。なお、コンテンツを暗号化して記録媒体に記録する方法としては、端末が保有する復号鍵に対応する暗号化鍵でコンテンツそのものを暗号化して記録する方法や、コンテンツをある鍵で暗号化して記録した上で、その鍵に対応する復号用の鍵を、端末が保有する復号鍵に対応する暗号化鍵で暗号化して記録する方法等がある。

- [0004] このとき、端末が保有する復号鍵は外部に露見しないように厳重に管理される必要があるが、不正者による端末内部の解析において、ある鍵が外部に暴露される危険性がある。ある鍵が一旦不正者に暴露されてしまうと、コンテンツを不正利用する記

録装置、再生装置、あるいはソフトウェアを作成し、インターネット等によりそれらを流布することが考えられる。このような場合、著作権者は一旦暴露された鍵では、次から提供するコンテンツを扱えないようにしたいと考える。これを鍵無効化技術と呼び、鍵無効化を実現するシステムとして、木構造と呼ばれる階層構造を利用した鍵無効化技術が、特許文献1、及び非特許文献1に開示されている。

[0005] 以下、非特許文献1に記載されている従来の鍵無効化技術について説明する。

まず、「Subset Difference」(以降、差分集合と呼ぶ)についての定義を行う。差分集合は、大きな木構造の集合から、それよりも小さな木構造の集合を取り除いたときの、各装置(リーフ)からなる集合と定義する。大きな木構造のルートと小さな木構造のルートの2つを定めることにより、差分集合は決定される。そして、各差分集合に対してそれぞれ復号鍵が割り当てられる。

[0006] さらに、コンテンツはコンテンツ鍵で暗号化されており、各装置は復号鍵を保持し、各装置が自身の保持する復号鍵を用いてコンテンツ鍵を求める際に必要とされるデータを鍵データと呼ぶ。一般的に、鍵データはコンテンツ共に配信され、コンテンツの配信に記録媒体を利用する場合は、鍵データは記録媒体に記録される。

無効化されない装置の集合を、差分集合でカバーすることによって、鍵データのサイズを削減することが可能となる。図42にその概念図を示す。図42において、大きな木構造T1000のルートをVi、小さな木構造T1001のルートをVjとした場合、×印をつけた2つのリーフに割り当てられた装置を無効化する集合は、木構造T1000から木構造T1001を取り除いた差分集合1001「Si, j」となる。さらに、必要となる鍵データは、前記差分集合Si, jに対応した1つの暗号化鍵Li, jを用いて暗号化された、1つの暗号化コンテンツ鍵となる。つまり、差分集合は、木構造T1000を示す概念的な図である概念図T1002から、木構造T1001を示す概念的な図である概念図T1003を除いた残りの部分に属するリーフの集合となる。

[0007] また、別の例として、装置数16の木構造において、装置3、装置4、装置13、装置15が無効化されている場合の差分集合、並びにコンテンツ鍵を暗号化するための暗号化鍵Si, jを図43に示す。例えば、装置9ー装置12は、V3をルートとする木構造T2000から、V7をルートとする木構造T2001を取り除いた差分集合2001「S3, 7」に

属する。図43においては、同一の差分集合 $S_{i,j}$ に属する装置は、共通の復号鍵を保持している。例えば、差分集合2002「 $S_2, 9$ 」に属する装置1、装置2、装置5ー装置8は、共通の復号鍵 $L_2, 9$ を保持し、差分集合2001「 $S_3, 7$ 」に属する装置9ー装置12は、共通の復号鍵 $L_3, 7$ を保持している。さらに、コンテンツ鍵は、 $L_2, 9$ 、 $L_3, 7$ 、 $L_{14}, 28$ 、 $L_{15}, 31$ でそれぞれ暗号化されるため、いずれの復号鍵も保持していない装置3、装置4、装置13、装置15は、コンテンツ鍵を復号することができず、コンテンツを扱うことができない。

[0008] ここで、各装置は、無効化される装置の位置関係に応じた復号鍵を保持する必要があり、その基本的な考え方は次の通りである。ある装置が差分集合 $S_{i,j}$ に対応した復号鍵 $L_{i,j}$ を保持する場合、その装置は、差分集合 $S_{i,k}$ に対応した復号鍵 $L_{i,k}$ も保持する。ただし、 V_k は V_j の部分集合とする。このとき、 $L_{i,k}$ は、 $L_{i,j}$ から計算で求めることができるようにするが、その逆は計算では求められないようにするため一方向性関数を利用する。

[0009] まず、木構造の各ノードに割り当てられる暗号化鍵(この暗号化鍵は、各装置が保持する復号鍵と対応する)について、図44に示す2分木の木構造T3000の例を用いて説明する。なお、図44は、合計8台の装置を管理する木構造T3000の一部を記載している。

図44に示す木構造T3000の各ノードには、それぞれ個別のTビットの「ラベル」と呼ばれる識別子が付与されている。そして、入力データ長Tビットに対して、3Tビットの乱数を生成する擬似乱数生成器Gを用意する。ラベル「A1」を擬似乱数生成器Gの入力とした場合に、出力される3Tビットのうち、前半Tビットをラベル3001「A1」の左下の子のラベルとし、真ん中のTビットをラベル3001「A1」のノードに対応する暗号化鍵とし、後半Tビットをラベル3001「A1」の右下の子のラベルとし、それぞれを「A1L」、「A1M」、「A1R」と表現する。図44では、各ノードには予めラベル「A1」、「A2」、「A3」、「A4」等が個別に割り当てられており、加えて上位のラベルから派生してきた新たなラベルが追加される。例えば、上から3層目のノード4001においては、当該ノードに予め割り当てられたラベル「A4」に加え、上位のラベル「A1」から派生したラベル「A1LL」、並びに同じく上位のラベル「A2」から派生したラベル「A2L」と計3

個のラベルが割り当てられことになる。さらに、各ノードに割り当てられる暗号化鍵の数は、当該ノードに割り当てられたラベルの数と等しくなるため、ノード4001には、A1LLM、A2LM、A4Mの計3つの暗号化鍵が割り当てられることになる。

[0010] ここで、差分集合 $S_{i,j}$ に対応する暗号化鍵 $L_{i,j}$ と、上記各ノードに割り当てられた暗号化鍵の関係を示す。ノード V_i とノード V_j を決定した場合、差分集合 $S_{i,j}$ に対応する暗号化鍵 $L_{i,j}$ は、ノード V_i に割り当てられたラベルから派生したラベルのうち、ノード V_j に追加されたラベルに対応する暗号化鍵となる。図44の例において、ノード V_i のラベルをA1、ノード V_j のラベルをA4とすると、暗号化鍵 $L_{i,j}$ はA1LLMとなる。

[0011] 次に、各装置に割り当てる復号鍵について説明する。ここでは、各装置には、ノードに割り当てられる複数のラベルが割り当てられるものとし、各装置は、装置内で、対応するラベルと擬似乱数生成器Gから復号鍵を生成するものとする。さらに、暗号化鍵と復号鍵が等しい秘密鍵暗号をその一例として説明する。

具体的には、各装置が割り当てられたリーフから、ルートに至る経路上に存在するノードにぶら下がるノードに着目して、当該ノードより上位に位置するノードから派生して割り当てられたラベルが、各装置に対して割り当てられる。

[0012] 例えば、図44に示す装置1に割り当てられるラベルは、A1LLR、A2LR、A4R、A1LR、A2R及びA1Rの計6つとなる。なお、ラベル「A3」、「A5」、「A7」は、それぞれが対応するノードに予め割り当てられているラベルであるため、装置1に対しては、割り当てられない。

各装置に割り当てられるラベルの総数は、装置の総数を t 台とした場合、 $0.5(\log_2 t)^2 + 0.5\log_2 t$ 個である。これは、各装置に割り当てられるラベルの数が、2層目に1個、3層目に2個、…、最下位層に $\log_2 t$ 個であることから、 $1+2+\dots+\log_2 t = 0.5(\log_2 t)^2 + 0.5\log_2 t$ となるからである。例えば、装置の総数が8台である場合には、各装置に割り当てられるラベルの数は、6つとなる。

[0013] 次に、図44を用いて、実際に装置を無効化する場合の例を説明する。

何れの装置も無効化されていない初期状態では、ラベル3002「A1L」、ラベル3003「A2R」に対応する鍵「A1LM」、及び「A1RM」を用いてコンテンツ鍵を暗号化する。全ての装置は、ラベル3002「A1L」、あるいはラベル3003「A1R」を保持してお

り、それらから、復号鍵「A1LM」、あるいは「A1RM」を生成することができる。従って、生成した復号鍵でコンテンツ鍵を復号することができ、さらには、復号したコンテンツ鍵を利用してコンテンツを復号することができる。

[0014] 装置1がハックされて、装置1が保持する全ての鍵が暴露された場合は、ラベル3001「A1」とラベル3004「A1LLL」を指定して、ラベル3001「A1」をルートとする大きな木構造T3000から、ラベル3004「A1LLL」の小さい木構造(リーフ)T3001を取り除く。そして、ラベル3004「A1LLL」に対応する暗号化鍵「A1LLLM」を用いてコンテンツ鍵を暗号化する。これにより、装置1は、擬似乱数生成器Gが一方向性であることから、自身が保持するラベルからは復号鍵「ALLLM」を生成することができないため、コンテンツ鍵を復号することができない。装置1以外の各装置は、ラベル3004「A1LLL」を保持する、又は保持しているラベルから、ラベル3004「A1LLL」を、擬似乱数生成器より生成することができる。つまり、装置1以外の各装置は、復号鍵「A1LLLM」を生成することができる。例えば、装置2は、ラベル3004「A1LLL」を保持しているため、保持しているラベル3004「A1LLL」から復号鍵「A1LLLM」を生成することができる。また、ラベル3006「A5」に対応するノードにぶら下がる2つのリーフ(図示していないが、例えば、装置3、装置4)は、ラベル3005「A1LL」を保持している。つまり、装置3及び装置4は、保持しているラベル3005「A1LL」から復号鍵「A1LLLM」を生成することができる。ラベル「A3」に対するノードが持つリーフ、つまり孫ノード(図示していないが、例えば、装置5ー装置8)は、ラベル3002「A1L」を保持している。つまり、装置5ー装置8は、ラベル3002「A1L」から復号鍵「A1LLLM」を生成することができる。

[0015] 以上により、非特許文献にて示されるシステムは、鍵無効化を実現している。

特許文献1:特開2002-281013号公報

非特許文献1:D. Naor, M. Naor, and J. Lotspiech, "Revocation and Tracing Schemes for Stateless Receivers", Proceedings of CRYPTO2001, LNCS2139, pp.41-62, 2001.

発明の開示

発明が解決しようとする課題

[0016] しかしながら、非特許文献1に開示されている従来の鍵無効化技術において、リーフを含む各ノードをルートする各部分木は、それぞれ独立した関係にある。なぜなら、各部分木のルートには、予めラベルが割り当てられており、割り当てられた各ラベルは、それぞれ独立した関係にあるからである。そのため、部分木に割り当てられたラベルから同一の部分木内に割り当てられたラベルを生成することはできるが、他の部分木に割り当てられたラベルを生成することはできない。したがって、従来の技術では、管理する装置数が増大すると、管理対象となる部分木の数が多くなる、つまり、各部分木のルートに対して、他のラベルから生成されることのないラベルを予め割り当てる際に、その個数が多くなるという課題がある。

[0017] 本発明は、前記従来の課題を解決するために、管理する装置に割り当てる鍵の基となる複数の固有情報のうち、他の固有情報から生成されることのない固有情報の個数を削減する管理装置、端末装置、著作権保護システム、記録媒体、関連付方法、関連付プログラム、プログラム記録媒体を提供することを目的とする。

課題を解決するための手段

[0018] 上記目的を達成するために、本発明は、複数の端末装置を識別する各装置識別子を木構造のリーフに配し、各装置識別子に、暗号化されたデータを復号する復号鍵の基となる固有情報を割り当て、管理する管理装置であって、前記木構造のリーフを除く各レイヤのノードにおいて、その配下に存する装置識別子の部分集合を求めて、生成する部分集合生成手段と、リーフのレイヤを除く最下位レイヤの部分集合をそっくり含む部分集合を直上位のレイヤから検索し、関連付ける第1関連付手段と、関連付先の部分集合をそっくり含む部分集合を同一レイヤ及び直上位のレイヤの何れかから検索し、関連付ける第2関連付手段と、最上位レイヤに至るまで、前記第2関連付手段が繰り返し処理するよう制御する第1制御手段と、前記最下位レイヤの部分集合の全てに対して、前記第1関連付手段、前記第2関連付手段、及び前記第1制御手段が繰り返し処理するよう制御する第2制御手段と、前記最下位レイヤの関連付元の部分集合に、固有情報を対応付けて、当該固有情報を、当該部分集合に含まれる装置識別子に割り当てる第1割当手段と、関連付けにより、レイヤにまたがって繋がった部分集合に、前記関連付元の部分集合に割り当てた固有情報から派生的

に求められる固有情報を対応付けて、当該固有情報を、当該部分集合に含まれる各装置識別子に割り当てる第2割当手段とを備えることを特徴とする。

発明の効果

[0019] 課題を解決するための手段に示した構成によると、管理装置は、第1関連付手段、第2関連付手段、第1制御手段、及び第2制御手段を用いて、最下位レイヤの部分集合から最上位レイヤの部分集合まで関連付けることができる。また、管理装置は、第2割当手段を用いて、関連付けにより繋がった部分集合に、最下位レイヤの部分集合に対応付けられた固有情報から派生的に求められる固有情報を対応付けることができる。従来の管理装置は、各レイヤの最小の要素数からなる各部分集合に対して、互いに関連性がない各固有情報を予め用意する必要があったが、本発明では、管理装置は、最下位レイヤの各部分集合のみに、互いに異なる各固有情報を用意するだけでよい。つまり、管理装置は、他の固有情報から生成されることのない固有情報を予め用意する際に、その個数を削減することができる。

[0020] ここで、前記第1関連付手段は、前記最下位レイヤの部分集合をそっくり含み、且つ最小の要素数からなる部分集合を検索し、前記最下位レイヤの部分集合を親ノードとし、検索した部分集合を子ノードとして、関連付け、前記第2関連付手段は、前記関連付先の部分集合をそっくり含み、且つ最小の要素数からなる部分集合を検索し、前記関連付先の部分集合を親ノードとし、検索した部分集合を子ノードとして、関連付け、前記第1制御手段は、最上位レイヤに至るまで、前記第2関連付手段が繰り返し処理するよう制御して、前記最下位レイヤの部分集合をルートする部分集合木を生成するとしてもよい。

[0021] この構成によると、管理装置は、最下位レイヤの部分集合をルートする部分集合木を生成することができる。これにより、管理装置は、部分集合間の関連付けを木構造にて管理することができる。

ここで、前記第1関連付手段は、前記最下位レイヤに対する各上位レイヤの各部分集合のうち、関連付けがなされた1以上の部分集合を除外し、残りの1以上の部分集合を用いて、最上位レイヤに至るまで、前記第2関連付手段が繰り返し処理するよう制御して、前記最下位レイヤの部分集合をルートする部分集合木を生成するとしても

よい。

- [0022] この構成によると、管理装置は、部分集合生成手段にて生成した各部分集合を1回のみ使用して、最下位レイヤの各部分集合をルートとする各部分集合木を生成することができる。

ここで、前記第2割当手段は、前記派生的に求められる固有情報を、前記関連付元の部分集合に対応付けされた固有情報から一方向性関数を用いて生成し、生成した固有情報を、関連付けにより繋がった部分集合に対応付けるとしてもよい。

- [0023] この構成によると、管理装置は、一方向性関数を用いて、最下位レイヤの部分集合に対応付けられた固有情報から、関連付けにより繋がった部分集合に対応付ける固有情報を生成することができる。

ここで、前記管理装置は、さらに、前記部分集合木のルートから1以上のリーフそれぞれに至る各経路において、固有情報を配布する配布対象の端末装置の識別子が、要素として初めて出現する部分集合が存在する場合に、前部分集合に対応付けられた固有情報を1以上取得する固有情報取得手段と、取得した固有情報と、固有情報に対応する部分集合を識別する集合識別情報とからなる1以上の組を、前記配布対象の端末装置へ配布する配布手段とを備えるとしてもよい。

- [0024] この構成によると、管理装置は、固有情報とその固有情報に対応する集合識別情報とからなる1以上の組を、配布対象の端末装置へ配布することができる。これにより、端末装置へ配布する固有情報の数を、従来よりも少なくすることができる。従来、各レイヤにおいて、部分集合間の関連付けを行い、レイヤ毎に、配布する固有情報を取得していたが、本発明によると、配布する固有情報が対応付けられた部分集合より上位レイヤに存在し、関連付けにより繋がった部分集合に対応付けられた固有情報を配布する必要が無い。なぜなら、配布する固有情報から、上位レイヤに存在し、関連付けにより繋がった部分集合に含まれる装置識別子に割り当てられた固有情報を派生的に求めることができるからである。これにより、管理装置は、配布対象の端末装置へ配布する固有情報の数を削減することができる。つまり、管理装置は、端末装置へ割り当てる鍵の数を削減することができる。

- [0025] ここで、前記固有情報取得手段は、部分集合木のルートからリーフに至る各経路か

ら、前記配布対象の端末装置の識別子が、要素として初めて出現する部分集合を検索し、前記部分集合を検出すると、前記検出した部分集合が未取得である場合に、前記検出した部分集合を取得する第1取得部と、第1取得部にて取得した前記部分集合に対応付けられた前記固有情報を取得する第2取得部と、前記各経路に対して行われるまで、前記第1及び第2取得部が繰り返し処理するよう制御する繰返制御部とを備えるとしてもよい。

[0026] この構成によると、管理装置は、繰返制御部により、部分集合木から、配布対象の端末装置へ配布する固有情報を1以上取得することができる。

ここで、前記管理装置は、さらに、前記部分集合木の構成要素である各部分集合と、前記各部分集合のそれぞれに対応付けられた前記固有情報とを記憶する領域を有する第1記憶手段と、前記部分集合木を構成する複数のノードと、各ノードの子ノードとを記憶する領域を有する第2記憶手段と、前記部分集合と、前記部分集合に対応付けられた固有情報とを対応付けて、前記第1記憶手段に書き込む第1書込手段と、前記部分集合木を構成する前記ノードと、前記ノードの子ノードとを対応付けて、前記第2記憶手段に書き込む第2書込手段とを備えるとしてもよい。

[0027] この構成によると、管理装置は、部分集合と部分集合に対応付けられた固有情報とを対応付けて記憶することができる。また、管理装置は、部分集合木を構成する複数のノードと、各ノードの子ノードとを対応付けて記憶することができる。

ここで、前記第1記憶手段は、前記部分集合と前記部分集合に対応付けられた固有情報とを1の組として、複数の組を記憶する第1テーブルを有しており、前記第2記憶手段は、前記ノードと前記ノードに対応する子ノードとを1の組として、複数の組を記憶する第2テーブルを有しており、前記第1書込手段は、前記部分集合と、前記部分集合に対応付けられた固有情報とからなる組を、前記第1テーブルに書き込み、前記第2書込手段は、前記ノードと、前記ノードの子ノードとからなる組を、前記第2記憶手段に書き込むとしてもよい。

[0028] この構成によると、管理装置は、第1テーブルを用いて、部分集合と部分集合に対応付けられた固有情報とを対応付けて記憶することができる。また、管理装置は、第2テーブルを用いて、部分集合木を構成する複数のノードと、各ノードの子ノードとを

対応付けて記憶することができる。

ここで、前記第2制御手段は、前記最下位レイヤの部分集合の全てに対して、前記第1関連付手段、前記第2関連付手段、及び前記第1制御手段が繰り返し処理するよう制御して、複数の部分集合木を生成し、前記第1記憶手段は、各部分集合木に含まれる各部分集合と、前記各部分集合のそれぞれに対応付けられた各固有情報とを記憶しており、前記管理装置は、さらに、前記複数の端末装置のうち、1以上の無効な端末を示す無効な識別子を記憶する領域を有する無効化識別子記憶手段と、前記無効化識別子記憶手段にて記憶されている内容に基づいて、前記第1記憶手段より1以上の部分集合を取得し、取得した各部分集合のそれぞれに対応付けられた各固有情報に基づいて、1以上の暗号化鍵を取得し、取得した各暗号化鍵を個別に用いて、コンテンツの利用に用いるメディア鍵を暗号し、前記1以上の暗号化鍵と同数の暗号化メディア鍵を生成する暗号化鍵生成手段と、前記暗号化メディア鍵と、前記暗号化メディア鍵に対する暗号化鍵の取得に用いられた部分集合を識別する基準識別情報とからなる1以上の組を、当該管理装置に装着された記録媒体へ書き込む第3書込手段とを備えるとしてもよい。

[0029] この構成によると、管理装置は、1以上の暗号化メディア鍵を生成し、生成した暗号化メディア鍵と、基準識別情報とからなる1以上の組を、装着された記録媒体に書き込むことができる。

ここで、前記管理装置は、さらに、無効な識別子を受け取り、受け取った無効な識別子を前記無効化識別子記憶手段へ書き込む無効化識別子受取手段を備えるとしてもよい。

[0030] この構成によると、管理装置は、無効な識別子を受け取り、受け取った無効な識別子を無効化識別子記憶手段へ書き込むことができる。

ここで、前記暗号化鍵は、前記復号鍵と同一の共通鍵であり、前記一方向性関数は、さらに、各固有情報から前記各固有情報に基づく各共通鍵を生成し、前記暗号化鍵生成手段は、前記無効化識別子記憶手段にて記憶されている無効な識別子を除く1以上の有効な識別子を最も多く含む部分集合を、前記第1記憶手段より取得する部分集合取得部と、全ての有効な識別子が、前記部分集合取得部にて取得される

1以上の部分集合の何れかに属するまで、前記部分集合取得部が繰り返し処理するよう制御する制御部と、前記一方向性関数を用いて、前記部分集合取得部にて取得した各部分集合のそれぞれに対応付けられた各固有情報から生成された1以上の共通鍵を取得する共通鍵取得部と、前記共通鍵取得部にて取得した各共通鍵を用いて、共通鍵の数と同数の暗号化メディア鍵を生成する暗号化部とを備えるとしてもよい。

- [0031] この構成によると、管理装置は、暗号化鍵である共通鍵を、一方向性関数を用いて、有効な識別子からなる部分集合に対応する固有情報から生成し、生成した共通鍵を用いて、暗号化メディア鍵を生成することができる。

ここで、前記基準識別情報は、前記暗号化メディア鍵に対する共通鍵の取得に用いられた部分集合であり、前記第3書込手段は、前記暗号化メディア鍵と、前記暗号化メディア鍵に対する共通鍵の取得に用いられた部分集合とからなる1以上の組を、前記記録媒体へ書き込み、前記配布手段は、前記取得した固有情報が対応付けられた部分集合を前記集合識別情報として、前記取得した固有情報と前記集合識別情報とからなる1以上の組を、前記配布対象の端末装置へ配布し、前記配布手段は、さらに、前記各部分集合木を示すデータ構造を配布するとしてもよい。

- [0032] この構成によると、管理装置は、基準識別情報を、暗号化鍵の取得に用いた部分集合とし、端末装置へ配布する集合識別情報を、配布する固有情報が対応付けられた部分集合とすることができる。さらに、管理装置は、端末装置へ、各部分集合木を示すデータ構造をも配布することができる。

ここで、前記管理装置は、さらに、部分集合に対して、前記部分集合が属する部分集合木のルートであるルート部分集合から、前記部分集合に至るまでの経路を示す生成経路と、前記ルート部分集合と示すルート識別子とを含む経路情報を取得する経路情報取得手段を備え、前記基準識別情報は、前記暗号化メディア鍵に対する暗号化鍵の取得に用いられた部分集合の経路情報であり、前記第3書込手段は、前記暗号化メディア鍵と、前記暗号化メディア鍵に対する暗号化鍵の取得に用いられた部分集合の経路情報とからなる1以上の組を、前記記録媒体へ書き込み、前記配布手段は、前記取得した固有情報に対する部分集合の経路情報を前記集合識別情

報として、前記取得した固有情報と前記集合識別情報とからなる1以上の組を、前記配布対象の端末装置へ配布するとしてもよい。

[0033] この構成によると、管理装置は、基準識別情報を、暗号化鍵の取得に用いた部分集合の経路情報とし、端末装置へ配布する集合識別情報を、配布する固有情報が対応付けられた部分集合の経路情報とすることができる。

また、本発明は、複数の端末装置を識別する各装置識別子を木構造にて管理する管理装置より、暗号化されたデータを復号する復号鍵の基となる固有情報が割り当てられる端末装置であって、前記管理装置は、前記木構造のリーフを除く各レイヤのノードにおいて、その配下に存する装置識別子の部分集合を求めて、生成し、リーフのレイヤを除く最下位レイヤの部分集合をそっくり含む部分集合を直上位のレイヤから検索し、関連付け、関連付先の部分集合をそっくり含む部分集合を同一レイヤ及び直上位のレイヤの何れかから検索し、関連付け、この関連付けを最上位レイヤに至るまで、前記第2関連付手段が繰り返し処理するよう制御し、前記最下位レイヤの部分集合の全てに対して、これらの処理が繰り返し処理するよう制御し、前記最下位レイヤの関連付元の部分集合に、固有情報を対応付けて、当該固有情報を、当該部分集合に含まれる装置識別子に割り当て、関連付けにより、レイヤにまたがって繋がった部分集合に、前記関連付元の部分集合に割り当てた固有情報から派生的に求められる固有情報を対応付けて、当該固有情報を、当該部分集合に含まれる各装置識別子に割り当てており、前記端末装置は、前記管理装置から予め配布された、関連付元の各部分集合に対応付けられた各固有情報のうち、当該端末装置の装置識別子を含む固有情報を記憶している固有情報記憶手段を備えることを特徴とする。

[0034] この構成によると、端末装置は、固有情報を記憶することができる。従来の管理装置は、レイヤ毎に各部分集合を関連付け、レイヤに存在する最小の要素数の部分集合に対して固有情報を対応付け、関連付けにて繋がった部分集合に対しては、最小の要素数の部分集合に割り当てた固有情報から派生的に求められる固有情報を対応付けていた。このため、従来の端末装置は、各レイヤにて関連付けされた部分集合の集まり毎に、当該端末装置の装置識別子を含む部分集合に対応付けられた固有情報を、記憶する必要があったが、本発明によると、管理装置は、各レイヤ間の関

連付けを行っているため、当該端末装置の端末識別子を含む部分集合に対応付けられた固有情報から派生的に求められる固有情報、つまり上位レイヤの部分集合に対応付けられた固有情報を記憶する必要がない。つまり、端末装置にて記憶する固有情報の数が削減される。

[0035] ここで、前記固有情報記憶手段は、さらに、記憶している前記固有情報が対応付けられた部分集合を識別する集合識別情報を記憶しており、前記端末装置は、さらに、前記集合識別情報が、当該端末装置が有効な装置であることを示すか否かを判断する判断手段と、前記判断手段による判断結果が肯定的である場合に、前記管理装置にて生成された各部分集合に対応付けられた各固有情報のうち特定の固有情報に基づく暗号化鍵により、メディア鍵が暗号化され、且つ前記暗号化鍵に関連する鍵関連情報と対応付けられた暗号化メディア鍵を取得する第1取得手段と、前記固有情報記憶手段にて記憶している前記固有情報を用いて、前記暗号化鍵に対応する復号鍵を取得する第2取得手段と、前記第2取得手段にて取得した前記復号鍵を用いて、前記取得手段にて取得した前記暗号化メディア鍵を復号して、前記メディア鍵を生成する復号手段とを備えるとしてもよい。

[0036] この構成によると、端末装置は、当該端末装置が有効な装置である場合に、暗号化メディア鍵及び復号鍵を取得し、取得した復号鍵を用いて、暗号化メディア鍵を復号して、メディア鍵を生成することができる。

ここで、前記特定の固有情報は、前記暗号化メディア鍵の生成時点で有効な端末装置の識別子を1以上含む部分集合に対応付けられた基準固有情報であり、前記暗号化鍵は、共通鍵であり、前記鍵関連情報は、前記基準固有情報が対応付けられた部分集合を識別する基準識別情報であり、前記暗号化メディア鍵は、前記基準識別情報と対応付けられており、前記判断手段は、前記固有情報記憶手段にて記憶している前記集合識別情報にて識別される部分集合から、前記基準識別情報にて識別される部分集合に至る経路が存在する場合に、前記集合識別情報は、当該端末装置が有効な装置であることを示す判断し、前記第1取得手段は、前記基準識別情報に対応する前記基準固有情報に基づく暗号化鍵により暗号化された前記暗号化メディア鍵を取得し、前記第2取得手段は、前記復号鍵を取得し、取得した前記

復号鍵を前記共通鍵とし、前記復号手段は、取得した前記共通鍵を用いて、前記暗号化メディア鍵を復号するとしてもよい。

- [0037] この構成によると、端末装置は、集合識別情報にて示される部分集合から、基準識別情報にて識別される部分集合に至る経路をもつ場合に、前記集合識別情報は、当該端末装置が有効な装置であることを示すと判断することができる。

ここで、前記管理装置は、前記最下位レイヤの部分集合をそっくり含み、且つ最小の要素数からなる部分集合を検索し、前記最下位レイヤの部分集合を親ノードとし、検索した部分集合を子ノードとして、関連付け、前記関連付先の部分集合をそっくり含み、最小の要素数からなり、且つ未関連付けである部分集合を検索し、前記関連付先の部分集合を親ノードとし、検索した部分集合を子ノードとして、関連付けて、前記最下位レイヤの部分集合をルートする部分集合木を生成し、前記固有情報記憶手段は、さらに、前記管理装置にて生成された前記部分集合木を構成するデータ構造を予め記憶しており、前記判断手段は、前記データ構造により構成される前記部分集合木を用いて、前記固有情報記憶手段にて記憶している前記固有情報が対応付けられた部分集合から、前記基準識別情報にて識別される部分集合に至る経路が存在するか否かを判断するとしてもよい。

- [0038] この構成によると、端末装置は、部分集合木を構成するデータ構造を用いて、集合識別情報にて示される部分集合から、基準識別情報にて識別される部分集合に至る経路が存在するか否かを判断することができる。

ここで、前記管理装置は、前記最下位レイヤの部分集合をそっくり含み、且つ最小の要素数からなる部分集合を検索し、前記最下位レイヤの部分集合を親ノードとし、検索した部分集合を子ノードとして、関連付け、前記関連付先の部分集合をそっくり含み、最小の要素数からなり、且つ未関連付けである部分集合を検索し、前記関連付先の部分集合を親ノードとし、検索した部分集合を子ノードとして、関連付けて、前記最下位レイヤの部分集合をルートする部分集合木を生成し、前記基準識別情報は、前記基準固有情報が対応付けられた基準部分集合に対して、前記許可集合木のルートから、当該基準部分集合に至るまでの第1生成経路を含み、前記集合識別情報は、前記固有情報が対応付けられた部分集合に対して、前記部分集合木のル

ートから、当該部分集合に至るまでの第2生成経路を含み、前記判断手段は、前記第2生成経路が前記第1生成経路に含まれる場合に、前記集合識別情報にて識別される部分集合から、前記基準識別情報にて識別される部分集合に至る経路が存在すると判断するとしてもよい。

[0039] この構成によると、端末装置は、基準識別情報に含まれる第1生成経路、及び各集合識別情報のそれぞれに含まれる第2生成経路を用いて、記憶している集合識別情報が、当該端末装置が有効な装置であることを示すか否かを判断することができる。

ここで、前記管理装置は、部分集合に対応付けられた固有情報を、一方向性関数に対する入力の情報として与え、前記固有情報に基づく共通鍵、及び前記固有情報から派生する固有情報を生成し、生成した固有情報を、入力の情報として与えた前記固有情報に対応付けられた部分集合と関連付けされた部分集合に対応付けて、関連付けされた部分集合に含まれる各装置識別子に、生成した固有情報を割り当て、前記第2取得手段は、前記一方向性関数と同一の関数を用いて、前記固有情報記憶手段にて記憶している前記固有情報から、前記固有情報に基づくデバイス鍵と、前記固有情報から派生する固有情報とを生成して、取得するデバイス鍵取得部と、前記基準固有情報に基づくデバイス鍵を取得するまで、前記デバイス鍵取得部にて取得した前記固有情報を、前記関数に対する次の入力の情報として与えて、前記デバイス鍵取得部の動作を繰り返すよう制御する繰返部と、前記デバイス鍵取得部にて取得した前記基準固有情報に基づくデバイス鍵を、前記共通鍵として取得する復号鍵取得手段とを備えるとしてもよい。

[0040] この構成によると、端末装置は、管理装置が有する一方向性関数と同一の関数を用いて、固有情報記憶手段にて記憶している固有情報から、基準固有情報に対応するデバイス鍵を共通鍵として取得することができる。

ここで、前記端末装置は、さらに、コンテンツを取得するコンテンツ取得手段と、コンテンツ鍵を取得するコンテンツ鍵取得手段と、前記コンテンツ鍵取得手段にて取得した前記コンテンツ鍵を、前記復号手段にて取得したメディア鍵を用いて、暗号化して暗号化コンテンツ鍵を生成する第1暗号化手段と、前記コンテンツ取得手段にて取得した前記コンテンツを、前記コンテンツ鍵取得手段にて取得したコンテンツ鍵を用

いて、暗号化して暗号化コンテンツを生成する第2暗号化手段と、前記暗号化コンテンツ鍵と、前記暗号化コンテンツとを、記録媒体へ書き込む書込手段とを備えるとしてもよい。

[0041] この構成によると、端末装置は、取得した共通鍵を用いて、コンテンツ鍵を暗号化して暗号化コンテンツ鍵を生成し、コンテンツ鍵を用いて、コンテンツを暗号化して暗号化コンテンツを生成し、生成した暗号化コンテンツ鍵及び暗号化コンテンツを記録媒体へ書き込むことができる。これにより、端末装置は、当該端末装置が有効な端末であると判断する場合に、暗号化コンテンツ鍵及び暗号化コンテンツを生成することができ、コンテンツに対する著作権が保護される。

[0042] ここで、前記書込手段は、前記暗号化コンテンツ鍵と、前記暗号化コンテンツとを、ネットワーク上に存在する装置が有する前記記録媒体へ、通信媒体を介して書き込むとしてもよい。

この構成によると、端末装置は、生成した暗号化コンテンツ鍵及び暗号化コンテンツを、通信媒体を介して、記録媒体へ書き込むことができる。

[0043] ここで、前記端末装置は、さらに、コンテンツ鍵が前記メディア鍵にて暗号化された暗号化コンテンツ鍵を取得する暗号化コンテンツ鍵取得手段と、コンテンツが前記コンテンツ鍵にて暗号化された暗号化コンテンツを取得する暗号化コンテンツ取得手段と、前記暗号化コンテンツ鍵取得手段にて取得した暗号化コンテンツ鍵を、前記メディア鍵を用いて、復号して、前記コンテンツ鍵を生成する第1復号手段と、前記暗号化コンテンツ取得手段にて取得した暗号化コンテンツを、前記コンテンツ鍵を用いて、復号して、前記コンテンツを生成する第2復号手段と、前記第2復号にて生成された前記コンテンツを再生する再生手段とを備えるとしてもよい。

[0044] この構成によると、端末装置は、取得した共通鍵を用いて、暗号化コンテンツ鍵を復号して、コンテンツ鍵を生成し、生成したコンテンツ鍵を用いて、暗号化コンテンツを復号して、コンテンツを生成し、生成したコンテンツを再生することができる。これにより、端末装置は、当該端末装置が有効な端末であると判断する場合に、暗号化コンテンツからコンテンツを生成し、生成したコンテンツを再生することができ、コンテンツに対する著作権が保護される。

[0045] ここで、前記暗号化コンテンツ鍵及び前記暗号化コンテンツは、記録媒体に記録されており、前記記録媒体は、当該端末装置に装着され、前記暗号化コンテンツ鍵取得手段は、前記記録媒体から、前記暗号化コンテンツ鍵を取得し、前記暗号化コンテンツ取得手段は、前記記録媒体から、前記コンテンツを取得するとしてもよい。

この構成によると、端末装置は、暗号化コンテンツ鍵及び暗号化コンテンツを、当該端末装置に装着された記録媒体から取得し、コンテンツを生成することができる。

[0046] ここで、前記暗号化コンテンツ鍵取得手段は、通信媒体を介して、前記暗号化コンテンツ鍵を取得し、前記暗号化コンテンツ取得手段は、通信媒体を介して、前記コンテンツを取得するとしてもよい。

この構成によると、端末装置は、暗号化コンテンツ鍵及び暗号化コンテンツを、通信媒体を介して取得し、コンテンツを生成することができる。

[0047] また、本発明は、複数の端末装置と、前記複数の端末装置を識別する各装置識別子を木構造のリーフに配し、各装置識別子に、暗号化されたデータを復号する復号鍵の基となる固有情報を割り当て、管理する管理装置とからなる著作権保護システムであって、前記管理装置は、前記木構造のリーフを除く各レイヤのノードにおいて、その配下に存する装置識別子の部分集合を求めて、生成する部分集合生成手段と、リーフのレイヤを除く最下位レイヤの部分集合をそっくり含む部分集合を直上位のレイヤから検索し、関連付ける第1関連付手段と、関連付先の部分集合をそっくり含む部分集合を同一レイヤ及び直上位のレイヤの何れかから検索し、関連付ける第2関連付手段と、最上位レイヤに至るまで、前記第2関連付手段が繰り返し処理するよう制御する第1制御手段と、前記最下位レイヤの部分集合の全てに対して、前記第1関連付手段、前記第2関連付手段、及び前記第1制御手段が繰り返し処理するよう制御する第2制御手段と、前記最下位レイヤの関連付元の部分集合に、固有情報を対応付けて、当該固有情報を、当該部分集合に含まれる装置識別子に割り当てる第1割当手段と、関連付けにより、レイヤにまたがって繋がった部分集合に、前記関連付元の部分集合に割り当てた固有情報から派生的に求められる固有情報を対応付けて、当該固有情報を、当該部分集合に含まれる各装置識別子に割り当てる第2割当手段とを備えることを特徴とする。

[0048] この構成によると、著作権保護システムの管理装置は、第1関連付手段、第2関連付手段、第1制御手段、及び第2制御手段を用いて、最下位レイヤの部分集合から最上位レイヤの部分集合まで関連付けることができる。また、管理装置は、第2割当手段を用いて、関連付けにより繋がった部分集合に、最下位レイヤの部分集合に対応付けられた固有情報から派生的に求められる固有情報を対応付けることができる。従来の管理装置は、各レイヤの最小の要素数からなる各部分集合に対して、互いに関連性がない各固有情報を予め用意する必要があったが、本発明では、管理装置は、最下位レイヤの各部分集合のみに、互いに異なる各固有情報を用意するだけでよい。つまり、管理装置は、他の固有情報から生成されることのない固有情報を予め用意する際に、その個数を削減することができる。

[0049] ここで、前記第1関連付手段は、前記最下位レイヤの部分集合をそっくり含み、且つ最小の要素数からなる部分集合を検索し、前記最下位レイヤの部分集合を親ノードとし、検索した部分集合を子ノードとして、関連付け、前記第2関連付手段は、前記関連付先の部分集合をそっくり含み、且つ最小の要素数からなる部分集合を検索し、前記関連付先の部分集合を親ノードとし、検索した部分集合を子ノードとして、関連付け、前記第1制御手段は、最上位レイヤに至るまで、前記第2関連付手段が繰り返し処理するよう制御して、前記最下位レイヤの部分集合をルートする部分集合木を生成するとしてもよい。

[0050] この構成によると、著作権保護システムの管理装置は、最下位レイヤの部分集合をルートする部分集合木を生成することができる。これにより、管理装置は、部分集合間の関連付けを木構造にて管理することができる。

ここで、前記第1関連付手段は、前記最下位レイヤに対する各上位レイヤの各部分集合のうち、関連付けがなされた1以上の部分集合を除外し、残りの1以上の部分集合を用いて、最上位レイヤに至るまで、前記第2関連付手段が繰り返し処理するよう制御して、前記最下位レイヤの部分集合をルートする部分集合木を生成するとしてもよい。

[0051] この構成によると、著作権保護システムの管理装置は、部分集合生成手段にて生成した各部分集合を1回のみ使用して、最下位レイヤの各部分集合をルートとする各

部分集合木を生成することができる。

ここで、前記第2割当手段は、前記派生的に求められる固有情報を、前記関連付元の部分集合に対応付けられた固有情報から一方向性関数を用いて生成し、生成した固有情報を、関連付けにより繋がった部分集合に対応付けるとしてもよい。

[0052] この構成によると、著作権保護システムの管理装置は、一方向性関数を用いて、最下位レイヤの部分集合に対応付けられた固有情報から、関連付けにより繋がった部分集合に対応付ける固有情報を生成することができる。

ここで、前記管理装置は、さらに、前記部分集合木のルートから1以上のリーフそれぞれに至る各経路において、固有情報を配布する配布対象の端末装置の識別子が、要素として初めて出現する部分集合が存在する場合に、前部分集合に対応付けされた固有情報を1以上取得する固有情報取得手段と、取得した固有情報と、固有情報に対応する部分集合を識別する集合識別情報とからなる1以上の組を、前記配布対象の端末装置へ配布する配布手段とを備えるとしてもよい。

[0053] この構成によると、著作権保護システムの管理装置は、固有情報とその固有情報に対応する集合識別情報とからなる1以上の組を、配布対象の端末装置へ配布することができる。これにより、端末装置へ配布する固有情報の数を、従来よりも少なくすることができる。従来、各レイヤにおいて、部分集合間の関連付けを行い、レイヤ毎に、配布する固有情報を取得していたが、本発明によると、配布する固有情報が対応付けられた部分集合より上位レイヤに存在し、関連付けにより繋がった部分集合に対応付けられた固有情報を配布する必要が無い。なぜなら、配布する固有情報から、上位レイヤに存在し、関連付けにより繋がった部分集合に対応付けられた固有情報を派生的に求めることができるからである。これにより、管理装置は、配布対象の端末装置へ配布する固有情報の数を削減することができる。つまり、管理装置は、端末装置へ割り当てる鍵の数を削減することができる。

[0054] ここで、前記管理装置は、さらに、前記部分集合木の構成要素である各部分集合と、前記各部分集合のそれぞれに対応付けされた前記固有情報とを記憶する領域を有する第1記憶手段と、前記部分集合木を構成する複数のノードと、各ノードの子ノードとを記憶する領域を有する第2記憶手段と、前記部分集合と、前記部分集合に

対応付けされた固有情報とを対応付けて、前記第1記憶手段に書き込む第1書込手段と、前記部分集合木を構成する前記ノードと、前記ノードの子ノードとを対応付けて、前記第2記憶手段に書き込む第2書込手段とを備えるとしてもよい。

- [0055] この構成によると、著作権保護システムの管理装置は、部分集合と部分集合に対応付けられた固有情報とを対応付けて記憶することができる。また、管理装置は、部分集合木を構成する複数のノードと、各ノードの子ノードとを対応付けて記憶することができる。

ここで、前記第2制御手段は、前記最下位レイヤの部分集合の全てに対して、前記第1関連付手段、前記第2関連付手段、及び前記第1制御手段が繰り返し処理するよう制御して、複数の部分集合木を生成し、前記第1記憶手段は、各部分集合木に含まれる各部分集合と、前記各部分集合のそれぞれに対応付けされた各固有情報とを記憶しており、前記管理装置は、さらに、前記複数の端末装置のうち、1以上の無効な端末を示す無効な識別子を記憶する領域を有する無効化識別子記憶手段と、前記無効化識別子記憶手段にて記憶されている内容に基づいて、前記第1記憶手段より1以上の部分集合を取得し、取得した各部分集合のそれぞれに対応付けされた各固有情報に基づいて、1以上の暗号化鍵を取得し、取得した各暗号化鍵を個別に用いて、コンテンツの利用に用いるメディア鍵を暗号し、前記1以上の暗号化鍵と同数の暗号化メディア鍵を生成する暗号化鍵生成手段と、前記暗号化メディア鍵と、前記暗号化メディア鍵に対する暗号化鍵の取得に用いられた部分集合を識別する基準識別情報とからなる1以上の組を、当該管理装置に装着された記録媒体へ書き込む第3書込手段とを備えるとしてもよい。

- [0056] この構成によると、著作権保護システムの管理装置は、1以上の暗号化メディア鍵を生成し、生成した暗号化メディア鍵と、基準識別情報とからなる1以上の組を、装着された記録媒体に書き込むことができる。

ここで、前記管理装置は、さらに、無効な識別子を受け取り、受け取った無効な識別子を前記無効化識別子記憶手段へ書き込む無効化識別子受取手段を備えるとしてもよい。

- [0057] この構成によると、著作権保護システムの管理装置は、無効な識別子を受け取り、

受け取った無効な識別子を無効化識別子記憶手段へ書き込むことができる。

ここで、前記暗号化鍵は、前記復号鍵と同一の共通鍵であり、前記一方向性関数は、さらに、各固有情報から前記各固有情報に基づく各共通鍵を生成し、前記暗号化鍵生成手段は、前記無効化識別子記憶手段にて記憶されている無効な識別子を除く1以上の有効な識別子を最も多く含む部分集合を、前記第1記憶手段より取得する部分集合取得部と、全ての有効な識別子が、前記部分集合取得部にて取得される1以上の部分集合の何れかに属するまで、前記部分集合取得部が繰り返し処理するよう制御する制御部と、前記一方向性関数を用いて、前記部分集合取得部にて取得した各部分集合のそれぞれに対応付けされた各固有情報から生成された1以上の共通鍵を取得する共通鍵取得部と、前記共通鍵取得部にて取得した各共通鍵を用いて、共通鍵の数と同数の暗号化メディア鍵を生成する暗号化部とを備えるとしてもよい。

[0058] この構成によると、著作権保護システムの管理装置は、暗号化鍵である共通鍵を、一方向性関数を用いて、有効な識別子からなる部分集合に対応する固有情報から生成し、生成した共通鍵を用いて、暗号化メディア鍵を生成することができる。

ここで、前記端末装置は、前記管理装置の配布手段にて予め配布された固有情報と、前記固有情報に対応付けされた部分集合を識別する集合識別情報とからなる1以上の組を記憶している固有情報記憶手段と、前記集合識別情報が、当該端末装置が有効な装置であることを示すか否かを判断する判断手段と、前記判断手段による判断結果が肯定的である場合に、前記記録媒体から暗号化メディア鍵を1個取得する第1取得手段と、前記固有情報記憶手段にて記憶している前記固有情報を用いて、前記暗号化鍵に対応する復号鍵を取得する第2取得手段と、前記第2取得手段にて取得した前記復号鍵を用いて、前記取得手段にて取得した前記暗号化メディア鍵を復号して、前記メディア鍵を生成する復号手段とを備えるとしてもよい。

[0059] この構成によると、著作権保護システムの端末装置は、固有情報を記憶することができる。従来の管理装置は、レイヤ毎に各部分集合に関連付け、レイヤに存在する最小の要素数の部分集合に対して固有情報に対応付け、関連付けにて繋がった部分集合に対しては、最小の要素数の部分集合に割り当てた固有情報から派生的に

求められる固有情報を対応付けていた。このため、従来の端末装置は、各レイヤにて関連付けされた部分集合の集まり毎に、当該端末装置の装置識別子を含む部分集合に対応付けられた固有情報を、記憶する必要があったが、本発明によると、管理装置は、各レイヤ間の関連付けを行っているため、当該端末装置の端末識別子を含む部分集合に対応付けられた固有情報から派生的に求められる固有情報、つまり上位レイヤの部分集合に対応付けられた固有情報を記憶する必要がない。つまり、端末装置にて記憶する固有情報の数が削減される。

[0060] また、端末装置は、当該端末装置が有効な装置である場合に、暗号化メディア鍵及び復号鍵を取得し、取得した復号鍵を用いて、暗号化メディア鍵を復号して、メディア鍵を生成することができる。

ここで、前記暗号化鍵は、共通鍵であり、前記判断手段は、前記固有情報記憶手段にて記憶している前記集合識別情報にて識別される部分集合から、前記基準識別情報にて識別される部分集合に至る経路が存在する場合に、前記集合識別情報は、当該端末装置が有効な装置であることを示す判断し、前記第1取得手段は、前記基準識別情報に対応する暗号化メディア鍵を取得し、前記第2取得手段は、前記復号鍵を取得し、取得した前記復号鍵を前記共通鍵とし、前記復号手段は、取得した前記共通鍵を用いて、前記暗号化メディア鍵を復号するとしてもよい。

[0061] この構成によると、著作権保護システムの端末装置は、集合識別情報にて示される部分集合から、基準識別情報にて識別される部分集合に至る経路をもつ場合に、前記集合識別情報は、当該端末装置が有効な端末装置であることを示すと判断することができる。

ここで、前記第2取得手段は、前記一方向性関数と同一の関数を用いて、前記固有情報記憶手段にて記憶している前記固有情報から、前記固有情報に基づくデバイス鍵と、前記固有情報から派生する固有情報とを生成して、取得するデバイス鍵取得部と、前記基準固有情報に基づくデバイス鍵を取得するまで、前記デバイス鍵取得部にて取得した前記固有情報を、前記関数に対する次の入力の情報として与えて、前記デバイス鍵取得部の動作を繰り返すよう制御する繰返部と、前記デバイス鍵取得部にて取得した前記基準固有情報に基づくデバイス鍵を、前記共通鍵として取得

する復号鍵取得手段とを備えるとしてもよい。

[0062] この構成によると、著作権保護システムの端末装置は、管理装置が有する一方向性関数と同一の関数を用いて、基準固有情報に対応するデバイス鍵を共通鍵として取得することができる。

また、本発明は、複数の端末装置を識別する各装置識別子を木構造のリーフに配し、各装置識別子に、暗号化されたデータを復号する復号鍵の基となる固有情報を割り当て、管理する管理装置であって、前記木構造のリーフを除く各レイヤのノードにおいて、その配下に存する装置識別子の部分集合を求めて、生成する部分集合生成手段と、同一レイヤにおいて存在する部分集合のうち、最小の要素数の部分集合を含む他の部分集合を、最小の要素数の部分集合とともに1つのグループにまとめるグループ生成手段と、同一レイヤの存在する最小の要素数の部分集合の全てに対して、前記グループ生成手段が繰り返し処理するよう制御する第1制御手段と、全てのレイヤに対して、前記グループ生成手段及び前記第1制御手段が繰り返し処理するよう制御する第2制御手段と、前記第2制御手段にて全てのレイヤに対して、処理を行った後、異なるレイヤ間において、下位レイヤのグループの何れかの部分集合を全て含む部分集合を有する上位レイヤのグループを、当該下位レイヤのグループと1のグループに統合する統合手段と、全てのレイヤにおいてグループの統合後に、残存する各グループ内の最小の要素数の各部分集合に対して、各固有情報に対応付けて、各部分集合に含まれる1以上の装置識別子に、対応付けられた各固有情報を割り当てる第1割当手段と、前記第1割当手段にて各固有情報を割り当てた最小の要素数の各部分集合と異なる各部分集合に対して、部分集合が属するグループに存在する最小の要素数の部分集合に対応付けされた固有情報から派生的に求められる固有情報に対応付けて、各部分集合に含まれる1以上の装置識別子に、対応付けられた固有情報を割り当てる第2割当手段とを備えることを特徴とする。

[0063] この構成によると、管理装置は、統合手段を用いて、最下位レイヤの部分集合から最上位レイヤの部分集合までの関連付けることができる。また、管理装置は、第2割当手段を用いて、関連付けにより繋がった部分集合に、最下位レイヤの部分集合に対応付けられた固有情報から派生的に求められる固有情報に対応付けることができ

る。従来の管理装置は、各レイヤの最小の要素数からなる各部分集合に対して、互いに関連性がない各固有情報を予め用意する必要があったが、本発明では、管理装置は、最下位レイヤの各部分集合のみに、互いに異なる各固有情報を用意するだけでよい。つまり、管理装置は、他の固有情報から生成されることのない固有情報を予め用意する際に、その個数を削減することができる。

図面の簡単な説明

- [0064] [図1]著作権保護システム10の全体の概要を示すブロック図である。
- [図2]鍵管理装置100の構成を示すブロック図である。
- [図3]木構造T100を示す概念図である。
- [図4]木構造テーブルT101のデータ構造の一例を示す一例である。
- [図5]デバイス鍵テーブルD100のデータ構造の一例を示す。
- [図6]相互関係テーブルD101のデータ構造の一例を示す。
- [図7]木構造T201、T202、T203及びT204を示す概念図である。
- [図8]木構造T205、T206、T207及びT208を示す概念図である。
- [図9]擬似乱数生成器G150の構成示す図である。
- [図10]デバイス鍵テーブルD100aのデータ構造の一例を示す。
- [図11]各部分集合の相互関係を示すテーブルである。
- [図12]各装置へ配布する鍵情報の合計数及び鍵情報を示すテーブルである。
- [図13]記録媒体200の構成を示すブロック図である。
- [図14]記録装置300の構成を示すブロック図である。
- [図15]鍵無効化データのみが記録された記録媒体200bを示す図である。
- [図16]再生装置400の構成を示すブロック図である。
- [図17]鍵無効化データ、暗号化コンテンツ鍵及び暗号化コンテンツが記録された記録媒体200cを示す図である。
- [図18]生成処理の動作概要を示す流れ図である。
- [図19]部分集合の生成処理を示す流れ図である。図20へ続く。
- [図20]部分集合の生成処理を示す流れ図である。図19から続く。
- [図21]デバイス鍵の生成処理を示す流れ図である。図22へ続く。

[図22]デバイス鍵の生成処理を示す流れ図である。図21から続き、図23へ続く。

[図23]デバイス鍵の生成処理を示す流れ図である。図22から続き、図24へ続く。

[図24]デバイス鍵の生成処理を示す流れ図である。図23から続き、図25へ続く。

[図25]デバイス鍵の生成処理を示す流れ図である。図24から続く。

[図26]鍵情報の取得処理を示す流れ図である。図27へ続く。

[図27]鍵情報の取得処理を示す流れ図である。図26から続く。

[図28]鍵無効化データの生成処理を示す流れ図である。

[図29]記録処理を示す流れ図である。

[図30]デバイス鍵の取得処理を示す流れ図である。

[図31]復号処理を示す流れ図である。

[図32]第1暗号化処理を示す流れ図である。

[図33]第2暗号化処理を示す流れ図である。

[図34]再生処理を示す流れ図である。

[図35]デバイス鍵の取得処理を示す流れ図である。

[図36]第1復号処理を示す流れ図である。

[図37]第2復号処理を示す流れ図である。

[図38]第3復号処理を示す流れ図である。

[図39]鍵無効化データのみが記録された記録媒体200bを示す図である。

[図40]各装置へ配布する鍵情報の合計数及び鍵情報を示すテーブルである。

[図41]木構造T100において、ノードE0、ノードE1及びノードE3それぞれをルートする各部分木の関連付けを示す図である。

[図42]従来技術における差分集合の概念を示す図である。

[図43]従来技術において、差分集合を示す一例である。

[図44]従来技術におけるラベルの割り当てを示す一例である。

符号の説明

- [0065] 10 著作権保護システム
- 100 鍵管理装置
- 101 装置情報格納部

- 102 情報格納部
- 103 情報生成部
- 104 配布部
- 105 無効化装置特定部
- 106 鍵無効化データ生成部
- 107 受付部
- 108 出力部
- 200 記録媒体
- 201 鍵無効化データ格納部
- 202 暗号化コンテンツ鍵格納部
- 203 暗号化コンテンツ格納部
- 300 記録装置
- 301 鍵情報格納部
- 302 コンテンツ格納部
- 303 コンテンツ鍵格納部
- 304 復号鍵生成部
- 305 復号部
- 306 第1暗号化部
- 307 第2暗号化部
- 308 受付部
- 309 入出力部
- 400 再生装置
- 401 鍵情報格納部
- 402 復号鍵生成部
- 403 第1復号部
- 404 第2復号部
- 405 第3復号部
- 406 再生部

407 受付部

408 読出部

420 モニタ

発明を実施するための最良の形態

[0066] 1. 第1の実施の形態

1. 1 著作権保護システム10の構成

本発明に係る実施の形態としての著作権保護システム10の構成を図1にて示す。

著作権保護システム10は、鍵管理装置100、記録媒体200、記録装置300a、300b、…、300c、及び再生装置400a、400b、…、400cからなる。

[0067] 鍵管理装置100は、DVD-RAM等のレコーダブルメディアであって、今だ何らの情報も記録されていない記録媒体200に、鍵無効化データを記録して、鍵無効化データが記録された記録媒体200を予め生成しておく。なお、何らの情報も記録されていない記録媒体200と、鍵無効化データが記録された記録媒体200とを区別するために、以降では、何らの情報も記録されていない記録媒体200を記録媒体200a、鍵無効化データが記録された記録媒体200を記録媒体200bと記述する。ここで、鍵無効化データとは、鍵管理装置100が予め記憶しているメディア鍵が暗号化された暗号化メディア鍵と、記録装置300a、300b、…、300c、再生装置400a、400b、…、400cのうち有効な装置がもつ装置識別子の集合からなる情報とを含んでいる。有効な装置がもつ装置識別子の集合は、各装置が有する装置識別子からなる集合の部分集合である。

[0068] また、鍵管理装置100は、記録装置300a、300b、…、300c及び再生装置400a、400b、…、400cのそれぞれに対して、1以上の鍵情報を割り当て、割り当てた1以上の鍵情報を、各装置へ予め配布しておく。ここで、鍵情報は、暗号化メディア鍵を復号するためのデバイス鍵を生成する基となるラベルと、ラベルを割り当てた装置が有する装置識別子の集合とを含む。

[0069] 記録装置300aは、デジタル化されたコンテンツを暗号化して、暗号化コンテンツを生成し、生成した暗号化コンテンツを、当該記録装置300aに装着された記録媒体200bに記録して、暗号化コンテンツが記録された記録媒体200を生成する。以降で

は、暗号化コンテンツが記録された記録媒体200を、記録媒体200cと記述する。ここで、コンテンツは、映像情報及び音声情報からなる。

[0070] 再生装置400aは、当該再生装置400aに装着された記録媒体200cから暗号化コンテンツを取り出し、取り出した暗号化コンテンツを復号して、元のコンテンツを得る。

なお、記録装置300b、・・・、300cは、記録装置300aと同様に動作し、再生装置400b、・・・、400cは、再生装置400aと同様に動作する。

[0071] また、以降において、部分集合を、当該部分集合に含まれる全ての要素を羅列して表記する。例えば、装置識別子1、2、3からなる部分集合を、部分集合「123」と表記し、装置識別子3、4からなる部分集合を、部分集合「34」と表記する。

1. 2 鍵管理装置100

鍵管理装置100は、図2に示すように、装置情報格納部101、情報格納部102、情報生成部103、配布部104、無効化装置特定部105、鍵無効化データ生成部106、受付部107及び出力部108から構成されている。

[0072] 鍵管理装置100は、具体的には、マイクロプロセッサ、ROM、RAM、ハードディスクユニット、ディスプレイユニット、キーボード、マウスなどから構成されるコンピュータシステムである。前記RAM又は前記ハードディスクユニットには、コンピュータプログラムが記憶されている。前記マイクロプロセッサが、前記コンピュータプログラムに従って動作することにより、鍵管理装置100は、その機能を達成する。

[0073] (1)装置情報格納部101

装置情報格納部101は、具体的にはハードディスクユニットから構成されており、図3に一例として示す2分木の木構造T100にて、各記録装置及び各再生装置のそれぞれを識別する装置識別子を管理するために、木構造T100を表現するためのデータ構造として、図4に示す木構造テーブルT101を記憶している。

[0074] 先ず、木構造T100について、説明する。図3は、一例として、記録装置及び再生装置の総数を8台とした場合の木構造T100を示している。木構造における各層をレイヤと呼び、レイヤ0のノードをルート、最下位レイヤ(図3の例では、レイヤ3)のノードをリーフと呼ぶ。また、各装置は、木構造のリーフに対して1対1に割り当てられる。リーフに割り当てられる情報は、各装置を識別する装置識別子である。木構造T100

には、8個のリーフに対して、それぞれ装置識別子1〜8が割り当てられている。

[0075] 例えば、ノードT130「E0」は、木構造T100のルートであり、ノードT131「E7」は、木構造T100のリーフであり、装置識別子「装置1」が割り当てられている。

次に、木構造テーブルT101について説明する。木構造テーブルT101は、親ノードと、それに対応する子ノードと装置識別子とからなる組を1以上、予め記憶している。親ノード名は、木構造T100が有するノードを示し、子ノード名は、親ノード名にて示されるノードの子ノードを示す。ただし、親ノードにて示されるノードがリーフである場合には、記号「ー」が記録されている。装置識別子は、各リーフに割り当てられた装置を識別する識別子であり、親ノード名にて示されるノードがリーフ以外である場合には、記号「ー」が記録されている。

[0076] 例えば、木構造テーブルT101にて示される組T170は、親ノード名T171「E0」、子ノード名T172「E1」、及び記号T173「ー」が記録された装置識別子からなる。また、組T175は、親ノード名T176「E7」、記号「ー」が記録された子ノード名、及び装置識別子T178「装置1」からなる。これにより、ノード「E0」は、子ノードとして「E1」をもち、ノード「E7」は、リーフであり、且つ装置識別子「装置1」が割り当てられていることが分かる。

[0077] 以上により、鍵管理装置100は、装置情報格納部101にて各装置識別子を管理、つまり、各記録装置及び各再生装置を管理することができる。

(2) 情報格納部102

情報格納部102は、具体的にはハードディスクユニットから構成されており、図5及び図6に一例として示すように、デバイス鍵テーブルD100及び相互関係テーブルD101を有している。

[0078] <デバイス鍵テーブルD100>

デバイス鍵テーブルD100は、有効な装置の装置識別子からなる部分集合と、その部分集合に対応付けられたラベル名と、ラベル名から生成されるデバイス鍵とからなる組を1以上有している。後述するように、情報生成部103によりデバイス鍵テーブルD100が生成され、情報格納部102に書き込まれる。なお、デバイス鍵テーブルD100は、記録装置及び再生装置の総数を8台とした場合において、情報生成部103に

て生成された結果を示す。

- [0079] デバイス鍵テーブルD100の各項目において、上段に部分集合、中段にラベル名、下段にデバイス鍵が記載される。例えば、項目D200において、上段に部分集合D201「1」、中段にラベルD202「A1」及び下段にデバイス鍵D203「K1」が記載される。

<相互関係テーブルD101>

相互関係テーブルD101は、図7及び図8に一例として示す部分集合の木構造T201、T202、T203、T204、T205、T206、T207及びT208に対応しており、各部分集合の木構造を表現するためのデータ構造を示す。後述するように、情報生成部103により各部分集合の木構造を表現するためのデータ構造が、相互関係テーブルD101として生成され、情報格納部102に書き込まれる。なお、相互関係テーブルD101は、記録装置及び再生装置の総数を8台とした場合において、情報生成部103にて生成された結果を示す。

- [0080] ここで、先ず各部分集合の木構造について説明する。

部分集合の木構造T201及びT205は、それぞれ部分集合「1」及び部分集合「5」をルートし、レイヤ0からレイヤ5までの6階層からなる。部分集合の木構造T201及びT205の各ノードは、デバイス鍵テーブルD100に記録されている部分集合のうち、そのノードに対する親ノードを含み、且つ要素数が最小となる部分集合である。

- [0081] 例えば、レイヤ1に存在するノードは、ルートである部分集合「1」を含み、要素数が最小の部分集合「12」となる。また、レイヤ2には、レイヤ1のノードである部分集合「12」を含み、要素数が最小の部分集合である部分集合「123」及び部分集合「124」をノードとしてもつ。

部分集合の木構造T202、T204、T206及びT208は、それぞれ部分集合「2」、部分集合「4」、部分集合「6」及び部分集合「8」をルートし、レイヤ0の1階層からなる。つまり、ルートから子ノードの関連付けがなされていない。

- [0082] 部分集合の木構造T203及びT207は、それぞれ部分集合「3」及び部分集合「7」をルートし、レイヤ0からレイヤ5までの6階層からなる。部分集合の木構造T203及びT207の各ノードは、デバイス鍵テーブルD100に記録されている部分集合のうち、

そのノードに対する親ノードを含み、要素数が最小の部分集合である。

以下、相互関係テーブルD101について説明する。

[0083] 相互関係テーブルD101は、部分集合の木構造T201、T202、T203、T204、T205、T206、T207及びT208に含まれるノードと同じ数のノード情報及びそのノード情報に対応するルート情報とを含んで構成されている。ここで、ノード情報は、親ノード及び子ノードからなる。各親ノードは、部分集合の木構造T201からT208を構成する各ノードに対応する部分集合を示し、子ノードは、当該親ノードより関連付けられる部分集合を示す。

[0084] なお、子ノードに記載されている「-」は、当該親ノードより関連付けされる部分集合が存在しないことを示す。また、親ノードにて同一の部分集合が2つ記録されている場合には、その部分集合に対する子ノードが2つ存在することを示している。このとき、上位に記録されている部分集合に対する子ノードは、左の子ノードを示し、下位に記録されている部分集合に対する子ノードは、右の子ノードを示す。親ノードにて、部分集合が1回のみ記録されている場合には、その部分集合に対する子ノードは1つであることを示しており、その子ノードは、右の子ノードを示す。

[0085] ルート情報は、対応する親ノードに記録されているノードがルートであるか否かを示す。親ノードに記録されているノードがルートである場合には、ルートであることを示す情報(ここでは、「ルート」)が記録され、ルートでない場合には、何も記録されない。

(3) 情報生成部103

情報生成部103は、一方向性関数であり、入力データ長Xビットに対して、3Xビットの乱数を生成する擬似乱数生成器G150を予め記憶している。なお、擬似乱数生成器G150に対して、値a1を入力した場合の結果と、値a1とは異なる値a2を入力した場合の結果とは異なる。

[0086] ここで、擬似乱数生成器G150の動作について、図9を用いて説明する。擬似乱数生成器G150は、データ長がXビットである入力値tを受け取ると、初期値Ivと、AES関数とを利用して、Xビットからなるt1を生成し、さらに、入力値tと、AES関数と、初期値Ivに生成した値t1を加算した値とを利用して、Xビットからなるt2を生成し、さらに、入力値tと、AES関数と、初期値Ivに生成した値t2を加算した値とを利用して、X

ビットからなる t_3 を生成し、生成した t_1 、 t_2 及び t_3 を結合して、3Xビットからなる値 $t_1 \mid \mid t_2 \mid \mid t_3$ を出力する。なお、記号「 $\mid \mid$ 」は結合を意味する。ここで、値 t_1 は、入力値 t に対するノードの子ノードを関連付ける際に、左の子ノードに対応するラベルであり、値 t_3 は、入力値 t に対するノードの子ノードを関連付ける際に、右の子ノードに対応するラベルであり、値 t_2 は、入力値 t に対するノードに割り当てられるデバイス鍵である。以降では、値 t_1 を左ラベル、値 t_3 を右ラベル、真ん中に位置する値 t_2 をデバイス鍵と呼ぶ。

- [0087] 情報生成部103は、デバイス鍵テーブルD100と同様の枠組みをもち、初期状態として何ら記録されていない作業用デバイス鍵テーブルを有している。つまり、作業用デバイス鍵テーブルは、デバイス鍵テーブルD100において、何ら記録されていない状態のテーブルである。

情報生成部103は、受付部107よりデバイス鍵を生成及びデバイス鍵テーブルD100へ格納する旨を示す生成指示を受け取る。

- [0088] 情報生成部103は、生成指示を受け取ると、装置情報格納部101にて、2分木により管理している全装置、つまり装置識別子から、有効な装置を示すの装置識別子からなる部分集合を1以上生成し、生成した各部分集合の関連付けを行い、相互関係テーブルD101を生成し、さらには、各部分集合に対して、ラベル及びデバイス鍵を生成し、生成したラベル及びデバイス鍵を割り当てたデバイス鍵テーブルD100を生成する。情報生成部103は、生成したデバイス鍵テーブルD100及び相互関係テーブルD101を、情報格納部102へ書き込む。

- [0089] <部分集合の生成>

情報生成部103は、装置情報格納部101にて管理している木構造の高さ T を取得し、作業用デバイス鍵テーブルの行カウンタ n に初期値0をセットする。

情報生成部103は、次の動作(a1)～(a6)を $i=0 \sim T-1$ までの間、繰り返す。

- [0090] (a1) 情報生成部103は、レイヤ i の存在するノードの数 N を取得する。次に、情報生成部103は、レイヤ i に存在するノードをルートとする部分木の高さ H を取得する。

(a2) 次の動作(a3)～(a6)を $j=0 \sim H-1$ までの間繰り返す。

(a3) 行カウンタ n に1を加算し、加算結果を n とする。

[0091] (a4) 次の動作(a5)及び(a6)を $k=1 \sim N$ までの間繰り返す。

(a5) レイヤ i の左から k 番目のノードをルートとする部分木を取得し、取得した部分木のリーフから、 2^j 個の端末識別子を除き、残り1以上の端末識別子からなる部分集合を1個以上生成する。これにより、無効な端末識別子を除いた有効な端末識別子からなる部分集合が生成される。ただし、複数の装置を除く場合、つまり複数の無効な装置識別子を除く場合には、無効な端末識別子全てが共通にもち、且つ無効な端末装置識別子だけがもつ上位ノードが存在する場合のみとする。

[0092] (a6) 生成した各部分集合を、作業用デバイス鍵テーブルの n 行目の未記録の列に対して、左から順に書き込む。

上記の動作により、情報生成部103は、作業用デバイス鍵テーブルから、部分集合のみが記録されたデバイス鍵テーブルD100aを生成する。以上により、上記の動作にて、部分集合を生成する部分集合生成部が構成されることになる。

[0093] なお、図10に示すデバイス鍵テーブルD100aは、図3に示す木構造T100を用いて、部分集合を生成した場合の結果である。以下に、図3に示す木構造T100を用いて、図10に示すデバイス鍵テーブルD100aを生成する具体的な動作について、説明する。

<デバイス鍵テーブルD100aの生成の具体例>

情報生成部103は、木構造T100の高さ $T=3$ を取得し、行カウンタ n に初期値0をセットする。

[0094] 情報生成部103は、以下の動作を $i=0 \sim 2$ まで繰り返す。

($i=0$ の場合)

情報生成部103は、動作(a)により、レイヤ $i=0$ の存在するノードの数 $N=1$ を取得する。次に、情報生成部103は、レイヤ $i=0$ に存在するノードをルートとする部分木の高さ $H=3$ を取得する。

[0095] 情報生成部103は、動作(a2)において、 $j=0 \sim 2$ までの間、動作(a3)～(a6)を繰り返す。

$j=0$ の場合、まず、動作(a3)において、行カウンタ $n(=0)$ に1加算し、 $n=1$ とする。次に、動作(a4)の繰り返しにより、動作(a5)及び(a6)を、 $k=1$ 回行う。

[0096] 動作(a5)において、レイヤ0の左から1番目をルートとする部分木、つまり木構造T100から、 $2^0 (=1)$ 個の端末識別子を除いた部分集合「1234567」、「1234568」、「1234578」、「1234678」、「1235678」、「1245678」、「1345678」及び「2345678」を生成し、動作(a6)において、生成した各部分集合を作業用デバイス鍵テーブルの $n=1$ 行目の未記録の列に対して、左から順に書き込む。

[0097] $j=1$ の場合、動作(a3)において、現時点での行カウンタ $n (=1)$ の値に1加算し、 $n=2$ とする。次に、動作(a4)の繰り返しにより、動作(a5)及び(a6)を、 $k=1$ 回行う。

動作(a5)において、木構造T100から、 $2^1 (=2)$ 個の端末識別子を除いた部分集合「123456」、「123478」、「125678」及び「345678」を生成し、動作(a6)において、生成した各部分集合を作業用デバイス鍵テーブルの $n=2$ 行目の未記録の列に対して、左から順に書き込む。

[0098] $j=2$ の場合、動作(a3)において、現時点での行カウンタ $n (=2)$ の値に1加算し、 $n=3$ とする。次に、動作(a4)の繰り返しにより、動作(a5)及び(a6)を、 $k=1$ 回行う。

動作(a5)において、木構造T100から、 $2^2 (=4)$ 個の端末識別子を除いた部分集合「1234」及び「5678」を生成し、動作(a6)において、生成した各部分集合を作業用デバイス鍵テーブルの $n=3$ 行目の未記録の列に対して、左から順に書き込む。

[0099] ($i=1$ の場合)

情報生成部103は、動作(a)により、レイヤ $i=1$ の存在するノードの数 $N=2$ を取得する。次に、情報生成部103は、レイヤ $i=1$ に存在するノードをルートとする部分木の高さ $H=2$ を取得する。

情報生成部103は、動作(a2)において、 $j=0-1$ までの間、動作(a3)〜(a6)を繰り返す。

[0100] $j=0$ の場合、動作(a3)において、現時点での行カウンタ $n (=3)$ の値に1加算し、 $n=4$ とする。次に、動作(a4)において、 $k=1-2$ までの間、動作(a5)及び(a6)を繰り返す。

$k=1$ の場合、動作(a5)において、レイヤ1の左から1番目をルートとする部分木から、 $2^0 (=1)$ 個の端末識別子を除いた部分集合「123」、「124」、「134」及び「234」を生成し、動作(a6)において、生成した各部分集合を作業用デバイス鍵テーブル

の $n=4$ 行目の未記録の列に対して、左から順に書き込む。

- [0101] $k=2$ の場合、動作(a5)において、レイヤ1の左から2番目をルートとする部分木から、 $2^0(=1)$ 個の端末識別子を除いた部分集合「567」、「568」、「578」及び「678」を生成し、動作(a6)において、生成した各部分集合をデバイス鍵テーブルD100の $n=4$ 行目の未記録の列に対して、左から順に書き込む。

$j=1$ の場合、動作(a3)において、現時点での行カウンタ $n(=4)$ の値に1加算し、 $n=5$ とする。次に、動作(a4)において、 $k=1\sim 2$ までの間、動作(a5)及び(a6)を繰り返す。

- [0102] $k=1$ の場合、動作(a5)において、レイヤ1の左から1番目をルートとする部分木から、 $2^1(=2)$ 個の端末識別子を除いた部分集合「12」及び「34」を生成し、動作(a6)において、生成した各部分集合を作業用デバイス鍵テーブルの $n=5$ 行目の未記録の列に対して、左から順に書き込む。

$k=2$ の場合、動作(a5)において、レイヤ1の左から2番目をルートとする部分木から、 $2^1(=2)$ 個の端末識別子を除いた部分集合「56」及び「78」を生成し、動作(a6)において、生成した各部分集合をデバイス鍵テーブルD100の $n=5$ 行目の未記録の列に対して、左から順に書き込む。

- [0103] ($i=2$ の場合)

情報生成部103は、動作(a)により、レイヤ $i=2$ の存在するノードの数 $N=4$ を取得する。次に、情報生成部103は、レイヤ $i=2$ に存在するノードをルートとする部分木の高さ $H=1$ を取得する。

情報生成部103は、動作(a2)において、 $j=0\sim H-1$ までの間、つまり、 $j=0$ の場合のみ、動作(a3)～(a6)を行う。

- [0104] $j=0$ の場合、動作(a3)において、現時点での行カウンタ $n(=5)$ の値に1加算し、 $n=6$ とする。次に、動作(a4)において、 $k=1\sim 4$ までの間、動作(a5)及び(a6)を繰り返す。

$k=1$ の場合、動作(a5)において、レイヤ1の左から1番目をルートとする部分木から、 $2^0(=1)$ 個の端末識別子を除いた部分集合「1」及び「2」を生成し、動作(a6)において、生成した各部分集合を作業用デバイス鍵テーブルの $n=6$ 行目の未記録

の列に対して、左から順に書き込む。

- [0105] $k=2$ の場合、動作(a5)において、レイヤ1の左から2番目をルートとする部分木から、 $2^0(=1)$ 個の端末識別子を除いた部分集合「3」及び「4」を生成し、動作(a6)において、生成した各部分集合を作業用デバイス鍵テーブルの $n=6$ 行目の未記録の列に対して、左から順に書き込む。

$k=3$ の場合、動作(a5)において、レイヤ1の左から3番目をルートとする部分木から、 $2^0(=1)$ 個の端末識別子を除いた部分集合「5」及び「6」を生成し、動作(a6)において、生成した各部分集合を作業用デバイス鍵テーブルの $n=6$ 行目の未記録の列に対して、左から順に書き込む。

- [0106] $k=4$ の場合、動作(a5)において、レイヤ1の左から4番目をルートとする部分木から、 $2^0(=1)$ 個の端末識別子を除いた部分集合「7」及び「8」を生成し、動作(a6)において、生成した各部分集合を作業用デバイス鍵テーブルの $n=6$ 行目の未記録の列に対して、左から順に書き込む。

(生成結果)

上記動作を行うことにより、情報生成部103は、図10に示すように、部分集合のみが記録されたデバイス鍵テーブルD100aを生成する。

- [0107] デバイス鍵テーブルD100aにおける1行目501、2行目502及び3行目503に記録される各部分集合は、木構造T100のレイヤ0に存在するノードT130「E0」をルートとする部分木から生成され、1行目501には、1つの端末識別子が除かれた部分集合、つまり7つの有効な端末識別子からなる部分集合が8個記録され、2行目502には、5つの有効な端末識別子からなる部分集合が4個記録され、3行目503には、4つの有効な端末識別子からなる部分集合が2個記録されている。

- [0108] また、4行目504及び5行目505に記録される各部分集合は、木構造T100のレイヤ1に存在する2つのノードそれぞれをルートする2つの部分木から生成され、4行目504には、3つの有効な端末識別子からなる部分集合が8個記録され、5行目505には、2つの有効な端末識別子からなる部分集合が4個記録されている。

6行目506に記録される8個の部分集合は、木構造T100のレイヤ2に存在する4つのノードそれぞれをルートする4つの部分木から生成される。

[0109] <デバイス鍵の生成>

情報生成部103は、相互関係テーブルD101と同様の枠組みをもち、初期状態として何ら記録されていない作業用相互関係テーブルを予め有している。つまり、作業用相互関係テーブルは、相互関係テーブルD101において、何ら記録されていない状態のテーブルである。

[0110] 情報生成部103は、装置情報格納部101にて管理している木構造の高さTを取得する。

情報生成部103は、次の動作(b1)〜(b11)を $h=1 \sim 2^T$ までの間、繰り返す。

(b1) Xビットからなる乱数 A_h を生成して、生成した乱数 A_h を、デバイス鍵テーブルD100aの $\{(T^2+T)/2\}$ 行、h列へ書き込む。これにより、情報生成部103は、デバイス鍵テーブルD100aの $\{(T^2+T)/2\}$ 行、h列の部分集合に対するラベルとして、乱数 A_h を割り当てることができる。

[0111] (b2) 擬似乱数生成器Gに、割り当てられたラベル、つまり乱数 A_h を入力値として与え、その出力として3Xビットの乱数を生成し、取得する。

(b3) 取得した3Xビットの乱数をXビットごとに分割し、左から2番目に位置するXビットを、割り当てられたラベルに対応するデバイス鍵「 K_m 」として、デバイス鍵テーブルD100aの $\{(T^2+T)/2\}$ 行、h列へ書き込む。また、両端に位置するXビットからなる2つの左ラベル及び右ラベルを、擬似乱数生成器Gへの入力に使用したラベル(つまり、乱数 A_h)に対する部分集合と対応付けて、一時的に記憶しておく。ただし、デバイス鍵を示す K_m の添字mは、初期値1から始まり、デバイス鍵が割り当てられる毎に1ずつ増加する値とし、 K_{m+1} は、 K_m の次に割り当てられるデバイス鍵であることを示す。

[0112] (b4) 次の動作(b5)〜(b11)を、 $i=\{(T^2+T)/2-1\} \sim 1$ までの間、繰り返す。

(b5) デバイス鍵テーブルD100aのi+1行目でデバイス鍵及びラベルが割り当てられた部分集合の個数Jを取得する。

(b6) 次の動作(b7)〜(b11)を、 $j=1 \sim J$ までの間、繰り返す。

[0113] (b7) デバイス鍵テーブルD100aのi+1行目でデバイス鍵及びラベルが割り当てられた左からj番目の部分集合 S_j を基準として、デバイス鍵テーブルD100aのi行目を

左から順に、部分集合 S_j を含み、且つデバイス鍵が未だ割り当てられていない部分集合を検索する。

(b8) 動作(b7)の検索により、部分集合 S_j を含み、デバイス鍵が未だ割り当てられていない部分集合が存在しない場合には、部分集合 S_j を親ノードとし、親ノードである部分集合 S_j と、その子ノードとなる部分集合が存在しないことを示す記号「-」とからなる組を、ノード情報として、作業用相互関係テーブル内の未記録である最上位の領域へ書き込む。つまり、部分集合 S_j は、親ノードの項目に書き込まれ、記号「-」は、子ノードの項目に書き込まれる。さらに、部分集合 S_j がルートである場合には、ルート情報に、ルートであることを示す情報(「ルート」)を記録し、ルートでない場合には、ルート情報には何も記録しない。部分集合 S_j がルートであるか否かの判断方法は、部分集合 S_j が記録されている行、つまり $i+1$ の値が、 $\{(T^2+T)/2\}$ であるか否かを判断すればよい。 $i+1$ の値が $\{(T^2+T)/2\}$ である場合には、部分集合 S_j は、デバイス鍵テーブルD100aの最下層に存在するため、部分集合 S_j に含まれる部分集合は存在しないことになる。つまり、部分集合 S_j を子ノードとする親ノードが存在しないことになり、部分集合 S_j がルートのノードとなる。

[0114] (b9) 動作(b7)の検索により、部分集合 S_j を含み、デバイス鍵が未だ割り当てられていない部分集合が1以上存在する場合には、デバイス鍵が未だ割り当てられていない1以上の部分集合のうち最大2つの部分集合を左から順に取得する。

(b10) 取得した部分集合が1つである場合には、部分集合 S_j に対応付けられ、一時的に記憶している左ラベル及び右ラベルのうち右ラベルを、取得した部分集合に対するラベルとして割り当て、割り当てた右ラベルを、デバイス鍵テーブルD100a内の取得した部分集合が記録されている欄へ書き込む。取得した部分集合が2つ(ここでは、 T_j 及び U_j とする)である場合には、2つの部分集合のうち左側に位置する部分集合 T_j に対するラベルとして、部分集合 S_j に対応付けられ、一時的に記憶している左ラベル及び右ラベルのうち左ラベルを割り当て、右側に位置する部分集合 U_j に対するラベルとして、部分集合 S_j に対応付けられ、一時的に記憶している左ラベル及び右ラベルのうち右ラベルを割り当てる。割り当てた左ラベルを、デバイス鍵テーブルD100a内の取得した部分集合 T_j が記録されている欄へ書き込み、割り当てた右ラベルを、取

得した部分集合 U_j が記録されている欄へ書き込む。

[0115] (b11) 取得した部分集合が1つである場合には、擬似乱数生成器Gに、取得した部分集合に割り当てられたラベル(つまり、一時的に記憶している右ラベル)を入力値として与え、その出力として3Xビットの乱数を生成して取得し、取得した3Xビットの乱数をXビットごとに分割し、左から2番目に位置するXビットを、割り当てられたラベルに対応するデバイス鍵「 K_m 」として、デバイス鍵テーブルD100a内の取得した部分集合が記録されている欄へ書き込む。さらに、情報生成部103は、当該動作(b11)にて取得した2つの左ラベル及び右ラベルを、擬似乱数生成器Gへの入力に使用したラベルに対する部分集合(つまり、動作(b9)にて取得した部分集合)と対応付けて、一時的に記憶しておく。さらに、部分集合 S_j を親ノードとし、取得した部分集合をその子ノードとして、作業用相互関係テーブル内の未記録である最上位の領域へ書き込む。さらに、部分集合 S_j がルートである場合には、ルート情報に、ルートであることを示す情報(「ルート」)を記録し、ルートでない場合には、ルート情報には何も記録しない。

[0116] (b12) 取得した部分集合が2つ(ここでは、左から順に取得した部分集合を、それぞれ部分集合 T_j 、部分集合 U_j とする。)である場合には、先ず、擬似乱数生成器Gに、取得した部分集合 T_j に割り当てられたラベル(つまり、一時的に記憶している左ラベル)を入力値として与え、その出力として3Xビットの乱数を生成して取得し、取得した3Xビットの乱数をXビットごとに分割し、左から2番目に位置するXビットを、割り当てられたラベルに対応するデバイス鍵「 K_m 」として、デバイス鍵テーブルD100a内の取得した部分集合 T_j が記録されている欄へ書き込む。さらに、情報生成部103は、左ラベルを入力値として、取得した2つの左ラベル及び右ラベルを、擬似乱数生成器Gへの入力に使用したラベルに対する部分集合 T_j と対応付けて、一時的に記憶しておく。さらに、部分集合 S_j を親ノードとし、取得した部分集合 T_j をその子ノードとして、作業用相互関係テーブル内の未記録である最上位の領域へ書き込む。さらに、部分集合 S_j がルートである場合には、ルート情報に、ルートであることを示す情報(「ルート」)を記録し、ルートでない場合には、ルート情報には何も記録しない。次に、擬似乱数生成器Gに、取得した部分集合 U_j に割り当てられたラベル(つまり、一時的に記憶

している右ラベル)を入力値として与え、その出力として3Xビットの乱数を生成して取得し、取得した3Xビットの乱数をXビットごとに分割し、左から2番目に位置するXビットを、割り当てられたラベルに対応するデバイス鍵「 $K_m + 1$ 」として、デバイス鍵テーブルD100a内の取得した部分集合 U_j が記録されている欄へ書き込む。さらに、情報生成部103は、右ラベルを入力値として、取得した2つの左ラベル及び右ラベルを、擬似乱数生成器Gへの入力に使用したラベルに対する部分集合 U_j と対応付けて、一時的に記憶しておく。さらに、部分集合 S_j を親ノードとし、取得した部分集合 U_j をその子ノードとして、作業用相互関係テーブル内の未記録である最上位の領域へ書き込む。さらに、部分集合 S_j がルートである場合には、ルート情報に、ルートであることを示す情報(「ルート」)を記録し、ルートでない場合には、ルート情報には何も記録しない。

[0117] 上記の動作により、情報生成部103は、図5に示すように、デバイス鍵テーブルD100aに記録されている全ての部分集合に対して、ラベルとデバイス鍵とを割り当てたデバイス鍵テーブルD100を生成することができ、さらには、作業用相互関係テーブルから相互関係テーブルD101をも生成することができる。

以下に、デバイス鍵テーブルD100aを用いて、情報生成部103が、ラベル及びデバイス鍵の生成し、生成したラベル及びデバイス鍵を割り当てる具体的な動作について、説明する。

[0118] <デバイス鍵の生成の具体例>

情報生成部103は、木構造T100の高さ $T = 3$ を取得する。

情報生成部103は、以下の動作を $h = 1 \sim 2^T$ まで繰り返す。

($h = 1$ の場合)

情報生成部103は、Xビットからなる乱数A1を生成して、生成した乱数A1を、6行、1列の部分集合「1」に対するラベルとして割り当て、割り当てられたラベルをデバイス鍵テーブルD100aの6行、1列へ書き込む。

[0119] 次に、情報生成部103は、擬似乱数生成器Gに、割り当てられたラベル、つまり乱数A1を入力値として与え、その出力として3Xビットの乱数を取得する。

情報生成部103は、取得した3Xビットの乱数をXビットごとに分割し、左から2番目

に位置するXビットを、割り当てられたラベルに対応するデバイス鍵「K1」として、デバイス鍵テーブルD100aの6行、1列へ書き込む。また、両端に位置するXビットからなる2つの左ラベル(ここでは、A1Lと表記する。)及び右ラベル(ここでは、A1Rと表記する。)を、擬似乱数生成器Gへの入力に使用したラベルに対する部分集合「1」と対応付けて、一時的に記憶しておく。

[0120] 情報生成部103は、動作(b5)～(b11)を、 $i=5-1$ までの間、繰り返す。

$i=5$ の場合、デバイス鍵テーブルD100aの6行目でデバイス鍵が割り当てられた部分集合の個数 $J=1$ を取得し、(b6)の繰り返しにより、動作(b8)～(b11)を、 $j=1$ 回行う。情報生成部103は、動作(b8)にて、デバイス鍵テーブルD100aの6行目でデバイス鍵が割り当てられた左から1番目の部分集合「1」を基準として、デバイス鍵テーブルD100aの5行目を左から順に、部分集合「1」を含み、且つデバイス鍵が未だ割り当てられていない部分集合を検索する。動作(b9)にて、部分集合「1」を含み、デバイス鍵が未だ割り当てられていない部分集合「12」を取得し、動作(b10)にて、一時的に記憶している右ラベル「A1R」を、取得した部分集合「12」に対するラベルとして割り当て、割り当てた右ラベルを、デバイス鍵テーブルD100a内の取得した部分集合「12」が記録されている欄へ書き込む。情報生成部103は、動作(b11)にて、擬似乱数生成器Gに、取得した部分集合「12」に割り当てられたラベル「A1R」を入力値として与え、その出力として3Xビットの乱数を取得し、取得した3Xビットの乱数をXビットごとに分割し、左から2番目に位置するXビットを、割り当てられたラベルに対応するデバイス鍵「K2」として、デバイス鍵テーブルD100a内の取得した部分集合「12」が記録されている欄へ書き込む。両端に位置するXビットからなる2つの左ラベル(A1RL)及び右ラベル(A1RR)を、擬似乱数生成器Gへの入力に使用したラベルに対する部分集合「12」と対応付けて、一時的に記憶しておく。さらに、部分集合「1」を親ノードとし、取得した部分集合をその子ノードとして、作業用相互関係テーブル内の未記録である最上位の領域へ書き込む。さらに、部分集合「1」はルートであるので、ルートであることを示す情報(「ルート」)を記録する。

[0121] $i=4$ の場合、デバイス鍵テーブルD100aの5行目でデバイス鍵が割り当てられた部分集合の個数 $J=1$ を取得し、(b6)の繰り返しにより、動作(b8)～(b11)を、 $j=1$

回行う。情報生成部103は、動作(b8)にて、デバイス鍵テーブルD100aの5行目でデバイス鍵が割り当てられた左から1番目の部分集合「12」を基準として、デバイス鍵テーブルD100aの4行目を左から順に、部分集合「12」を含み、且つデバイス鍵が未だ割り当てられていない部分集合を検索する。動作(b9)にて、部分集合「1」を含み、デバイス鍵が未だ割り当てられていない部分集合「123」及び「124」を取得し、動作(b10)にて、2つの部分集合「123」及び「124」のうち左側に位置する部分集合「123」に対するラベルとして、一時的に記憶している左ラベル(A1RL)を割り当て、右側に位置する部分集合「124」に対するラベルとして、一時的に記憶している右ラベル(A1RR)を割り当てる。割り当てた左ラベルを、デバイス鍵テーブルD100a内の取得した部分集合「123」が記録されている欄へ書き込み、割り当てた右ラベルを、取得した部分集合「124」が記録されている欄へ書き込む。

- [0122] 情報生成部103は、動作(b12)にて、先ず、擬似乱数生成器Gに、取得した部分集合「123」に割り当てられたラベル(A1RL)を入力値として与え、その出力として3Xビットの乱数を取得し、取得した3Xビットの乱数をXビットごとに分割し、左から2番目に位置するXビットを、割り当てられたラベルに対応するデバイス鍵「K3」として、デバイス鍵テーブルD100a内の取得した部分集合「123」が記録されている欄へ書き込む。両端に位置するXビットからなる2つの左ラベル(A1RLL)及び右ラベル(A1RRL)を、擬似乱数生成器Gへの入力に使用したラベルに対する部分集合「123」と対応付けて、一時的に記憶しておく。さらに、部分集合「12」を親ノードとし、取得した部分集合「123」をその子ノードとして、作業用相互関係テーブル内の未記録である最上位の領域へ書き込む。なお、部分集合「12」はルートではないため、ルート情報には何も記録しない。次に、擬似乱数生成器Gに、取得した部分集合「124」に割り当てられたラベル(A1RR)を入力値として与え、その出力として3Xビットの乱数を取得し、取得した3Xビットの乱数をXビットごとに分割し、左から2番目に位置するXビットを、割り当てられたラベルに対応するデバイス鍵「K4」として、デバイス鍵テーブルD100a内の取得した部分集合「124」が記録されている欄へ書き込む。両端に位置するXビットからなる2つの左ラベル(A1RRL)及び右ラベル(A1RRR)を、擬似乱数生成器Gへの入力に使用したラベルに対する部分集合「124」と対応付けて、一時的に

記憶しておく。さらに、部分集合「12」を親ノードとし、取得した部分集合「124」をその子ノードとして、作業用相互関係テーブル内の未記録である最上位の領域へ書き込む。なお、部分集合「12」はルートではないため、ルート情報には何も記録しない。

[0123] $i=3, 2$ 及び 1 に対しても、上記に示す動作を行うことにより、部分集合「1」をルートとする木構造 T100 を示すデータ構造、及びデバイス鍵「K1」〜「K11」と、各デバイス鍵に対応するラベルを取得することができる。

また、 $h=2, 3, 4, 5, 6, 7$ 及び 8 のそれぞれに対しても、上記に示す動作を行うことにより、部分集合「2」、「3」、「4」、「5」、「6」、「7」及び「8」をルートとする木構造 T202、T203、T204、T205、T206、T207 及び T208 を示すデータ構造、及びデバイス鍵「K12」〜「K34」と、各デバイス鍵に対応するラベルを取得することができる。

[0124] (生成結果)

上記動作を行うことにより、情報生成部 103 は、図 5 及び図 6 に示すように、デバイス鍵テーブル D100 及び相互関係テーブル D101 を生成する。

デバイス鍵テーブル D100 の 1 行目には、1 つの端末識別子が除かれた部分集合、つまり 7 つの有効な端末識別子からなる部分集合、それら部分集合に割り当てられたラベル及びデバイス鍵が記録され、2 行目には、5 つの有効な端末識別子からなる部分集合、それら部分集合に割り当てられたラベル及びデバイス鍵が記録され、3 行目には、4 つの有効な端末識別子からなる部分集合、それら部分集合に割り当てられたラベル及びデバイス鍵が記録されている。以下、4 行目、5 行目及び 6 行目には、それぞれ 3 つの有効な端末識別子、2 つの有効な端末識別子及び 1 つの有効な端末識別子からなる部分集合、それら部分集合に割り当てられたラベル及びデバイス鍵が記録されている。

[0125] また、相互関係テーブル D101 には、部分集合「1」、「2」、「3」、「4」、「5」、「6」、「7」及び「8」をルートとする木構造 T201、T202、T203、T204、T205、T206、T207 及び T208 を示すデータ構造が記録されている。

ここで、上記動作により各部分集合が関連付けられた状態を、図 11 のテーブルにて示す。テーブルの各要素は、部分集合であり、矢印は、2 つの部分集合が関連付けられる方向を示す。部分集合の関連付けは、親ノードである部分集合に対応する

ラベルから、その子ノードに対応するラベルが生成できることを意味している。

[0126] 例えば、部分集合510「1」から部分集合511「12」へ、矢印512により関連付けがなされている。これは、部分集合510「1」を親ノードとし、部分集合511「12」をその子ノードとして2つのノードが関連付けられており、これは、部分集合510「1」のラベル「A1」から、部分集合511「12」のラベル「A1R」を生成することができることを意味している。また、部分集合511「12」から部分集合513「123」及び部分集合514「124」へ、それぞれ矢印515及び516により関連付け、つまり、部分集合511「12」を親ノードとし、部分集合513「123」及び部分集合514「124」をその子ノードとして関連付けがなされている。

[0127] ここで、部分集合の関連付けを行うことにより、ラベルの関連付けが行われていることがわかる。なぜなら、部分集合の関連付けにより、親ノードとなる部分集合に割り当てられたラベルから、子ノードに割り当てられた部分集合に対するラベルを、一方向性関数である擬似乱数生成器G150を用いて、生成するからである。

(4) 配布部104

配布部104は、装置へ配布するラベル及びそのラベルに対応する部分集合を、一時的に記憶する鍵情報記憶領域を備えている。

[0128] 配布部104は、受付部107より、鍵情報の配布指示及び配布する装置を示す装置識別子とを受け取る。

配布部104は、配布指示及び装置識別子を受け取ると、受け取った装置識別子に対する装置へ、配布するラベルと、そのラベルに対応する部分集合とを含む鍵情報を1以上生成して取得する。なお、鍵情報の取得方法については、後述する。

[0129] 配布部104は、情報格納部102にて記憶している相互関係テーブルD101を読み出す。

配布部104は、取得した1以上の鍵情報と、読み出した相互関係テーブルD101とを受け付けた装置識別子に対応する装置へ配布する。

ここで、配布方法に一例を、以下に説明する。配布部104は、当該鍵管理装置100に装着された配布用の記録媒体に、受け付けた装置識別子と、取得した1以上の鍵情報と、読み出した相互関係テーブルD101とを書き込む。鍵管理装置100を管

理する業者は、装置識別子と、1以上の鍵情報と、相互関係テーブルD101とが書き込まれた記録媒体を、装置を製造する製造業者へ配布する。製造業者は、記録媒体を受け取ると、記録媒体に記録されている装置識別子に対応する装置の製造中に、記録媒体に記録されている1以上の鍵情報と、相互関係テーブルとを読み出し、読み出した1以上の鍵情報と相互関係テーブルD101とを製造中の装置へ書き込む。これにより、装置識別子に対応する装置へ、1以上の鍵情報と相互関係テーブルD101とを配布することができる。

[0130] <鍵情報の取得>

ここでは、鍵情報の取得の動作について説明する。

配布部104は、配布指示と、配布する装置の装置識別子を受け取ると、相互関係テーブルD101にて管理されている木構造の個数Yを取得する。

配布部104は、次の動作(c1)～(c6)を、 $i=1\sim Y$ までの間繰り返す。

[0131] (c1)配布部104は、相互関係テーブルD101にて上位からi番目に管理されている木構造Viを示すデータ構造を取得する。

(c2)取得したデータ構造から、子ノードを持たないノード(つまり、リーフ)の数Pを取得する。

(c3)配布部104は、次の動作(c4)～(c6)を、 $p=1\sim P$ までの間繰り返す。

[0132] (c4)配布部104は、取得したデータ構造の親ノードの項目から、子ノードを持たない、上位p番目のノードWp(つまり、Wpはリーフとなる。)を取得し、木構造Viのルートを開始点として、リーフWpまでに至る経路に対して、受け取った装置識別子を含む部分集合が出現する最初のノード(部分集合)を検索する。

(c5)動作(c4)の検索により、ノードを検出すると、検出したノードが鍵情報記憶領域に記憶済みであるか否かを判断する。

[0133] (c6)記憶済みでないと判断する場合には、配布部104は、検出したノード、つまり部分集合に対応するラベルをデバイス鍵テーブルD100から読み出し、読み出したラベルと検出した部分集合とを含む鍵情報を生成して取得し、取得した鍵情報を鍵情報記憶領域へ記憶する。記憶済みであると判断する場合には、鍵情報の生成及び鍵情報記憶領域へ記憶は行わない。

[0134] 上記の動作により、配布部104は、受け取った装置識別子に対応する装置へ配布するラベル及び部分集合を含む鍵情報を全て鍵情報記憶領域へ記憶する。配布部104は、相互関係テーブルD101を読み出し、読み出した相互関係テーブルD101と鍵情報記憶領域にて記憶している全ての鍵情報とを、配布対象の装置へ配布する。

配布部104は、相互関係テーブルD101と全ての鍵情報とを、受け取った装置識別子をもつ装置へ配布した後、鍵情報記憶領域にて記憶している全ての鍵情報を消去する。なお、ここで、配布とは、例えば、配布用の記録媒体に、受け付けた装置識別子と、鍵情報記憶領域にて記憶している1以上の鍵情報と、相互関係テーブルD101との書き込みが完了したことをいう。

[0135] <鍵情報の取得の具体例>

以下に、デバイス鍵テーブルD100及び相互関係テーブルD101を用いて、装置識別子1が与えられた場合における、鍵情報の取得の具体的な動作について、説明する。

配布部104は、配布指示と装置識別子「1」とを受け取ると、相互関係テーブルD101にて管理されている木構造の個数8を取得する。

[0136] 配布部104は、動作(c1)～(c6)を、 $i=1\sim 8$ までの間繰り返す。

($i=1$ の場合)

配布部104は、相互関係テーブルD101にて上位から1番目に管理されている木構造V1を示すデータ構造を取得する。ここでは、木構造V1を示すデータ構造は、相互関係テーブルD101の1行目から15行目までに示されるデータ構造D300である。

[0137] 配布部104は、取得したデータ構造から、子ノードを持たないノード(つまり、リーフ)の数5を取得する。

配布部104は、動作(c4)～(c6)を、 $p=1\sim 5$ までの間繰り返す。

$p=1$ の場合において、配布部104は、取得したデータ構造の親ノードの項目から、子ノードを持たない、上位1番目のノードW1(ここでは、図6における部分集合D302「124」となる。)を取得し、木構造V1のルートを起点として、リーフW1までに至る経

路に対して、受け取った装置識別子を含む部分集合が出現する最初のノード(部分集合)を検索する。配布部104は、検索により、ノード1(ここでは、図6における部分集合D301「1」)を検出し、検出した部分集合D301「1」が既に鍵情報記憶領域に記憶済みであるか否かを判断する。

- [0138] 配布部104は、記憶済みでないと判断し、検出した部分集合D301「1」に対応するラベルD202「A1」をデバイス鍵テーブルD100から読み出し、読み出したラベルD202「A1」と、検出した部分集合D301「1」とを含む鍵情報を生成して取得し、取得した鍵情報を鍵情報記憶領域へ記憶する。

p=2の場合において、配布部104は、取得したデータ構造の親ノードの項目から、子ノードを持たない、上位2番目のノードW2(ここでは、部分集合D303「1234567」となる。)を取得し、木構造V1のルートを起点として、リーフW2までに至る経路に対して、受け取った装置識別子を含む部分集合が出現する最初のノード(部分集合)を検索して、ノード1(ここでは、部分集合D301「1」)を検出するが、鍵情報記憶領域に記憶済みであると判断し、鍵情報の生成及び鍵情報記憶領域への記憶は行わない。

- [0139] p=3〜5に対しても同様に、配布部104は、ノード1を検出するが、記憶済みであると判断し、鍵情報の生成及び鍵情報記憶領域への記憶は行わない。

(i=2の場合)

配布部104は、相互関係テーブルD101にて上位から2番目に管理されている木構造V2を示すデータ構造を取得する。ここでは、木構造V2を示すデータ構造は、相互関係テーブルD101の16行目からなるデータ構造D310である。

- [0140] 配布部104は、取得したデータ構造D310から、子ノードを持たないノード(つまり、リーフ)の数1を取得する。

配布部104は、動作(c4)〜(c6)を、p=1回、行う。

配布部104は、取得したデータ構造の親ノードの項目から、子ノードを持たない、上位1番目のノードW1(ここでは、部分集合D311「2」となる。)を取得し、木構造V2のルートを起点として、リーフW1までに至る経路に対して、受け取った装置識別子を含む部分集合が出現する最初のノード(部分集合)を検索する。配布部104は、検索により、ノードは検出しない。

[0141] (i=3の場合)

配布部104は、相互関係テーブルD101にて上位から3番目に管理されている木構造V3を示すデータ構造を取得する。ここでは、木構造V3を示すデータ構造は、相互関係テーブルD101の17行目から21行目までからなるデータ構造D320である。

配布部104は、取得したデータ構造から、子ノードを持たないノード(つまり、リーフ)の数2を取得する。

[0142] 配布部104は、動作(c4)〜(c6)を、p=1〜2までの間繰り返す。

p=1の場合において、配布部104は、取得したデータ構造の親ノードの項目から、子ノードを持たない、上位1番目のノードW1(ここでは、部分集合D321「134」となる。)を取得し、木構造V3のルートを起点として、リーフW1までに至る経路に対して、受け取った装置識別子を含む部分集合が出現する最初のノード(部分集合)を検索する。配布部104は、検索により、ノード(ここでは、部分集合D321「134」)を検出し、検出した部分集合D321「134」が、鍵情報記憶領域に記憶済みであるか否かを判断する。

[0143] 配布部104は、記憶済みでないと判断し、検出した部分集合D321「134」に対応するラベルD204「A3RL」をデバイス鍵テーブルD100から読み出し、読み出したラベルD204「A3RL」と、検出した部分集合D321「134」とを含む鍵情報を生成して取得し、取得した鍵情報を鍵情報記憶領域へ記憶する。

p=2の場合において、配布部104は、取得したデータ構造の親ノードの項目から、子ノードを持たない、上位2番目のノードW2(ここでは、部分集合D322「234」となる。)を取得し、木構造V3のルートを起点として、リーフW2までに至る経路に対して、受け取った装置識別子を含む部分集合が出現する最初のノード(部分集合)を検索する。配布部104は、検索により、ノードは検出しない。

[0144] (i=4の場合)

配布部104は、相互関係テーブルD101にて上位から4番目に管理されている木構造V4を示すデータ構造を取得する。ここでは、木構造V4を示すデータ構造は、相互関係テーブルD101の22行目からなるデータ構造D330である。

配布部104は、取得したデータ構造から、子ノードを持たないノード(つまり、リーフ)の数1を取得する。

[0145] 配布部104は、動作(c4)〜(c6)を、 $p=1$ 回行う。

配布部104は、取得したデータ構造の親ノードの項目から、子ノードを持たない、上位1番目のノードW1(ここでは、部分集合D331「4」となる。)を取得し、木構造V4のルートを起点として、リーフW1までに至る経路に対して、受け取った装置識別子を含む部分集合が出現する最初のノード(部分集合)を検索する。配布部104は、検索により、ノードは検出しない。

[0146] 配布部104は、以降、 $i=5\sim 8$ まで、上記にて示す動作を行い、部分集合「125678」及びラベル「A5RLRL」を含む鍵情報と、部分集合「1345678」及びラベル「A5RLRRL」を含む鍵情報とを生成し、鍵情報記憶領域へ記憶する。

以上により、配布部104は、受け取った装置識別子に対応する装置へ配布するラベル及び部分集合からなる鍵情報を全て鍵情報記憶領域へ記憶する。配布部104は、相互関係テーブルD101を情報格納部102から読み出し、読み出した相互関係テーブルD101と、鍵情報記憶領域にて記憶している全ての鍵情報とを、装置識別子1を有する装置へ配布する。

[0147] 配布部104は、相互関係テーブルD101と取得した全ての鍵情報とを、装置識別子1をもつ装置へ配布した後、鍵情報記憶領域にて記憶している全ての鍵情報を消去する。

また、図12に示すテーブルD400にて、装置1から装置8のそれぞれに配布する鍵情報、つまり各装置が保持する鍵情報の合計数及び鍵情報を示す。なお、図12では、鍵情報を、鍵情報に含まれる部分集合の要素の数が少ないものから順に、左より記述している。例えば、従来の装置が保持するラベルの数は、各装置とも均一に6個保持していたが、装置1が保持する鍵情報の個数は4個であり、従来よりも2個少なくなる。合計の項目における括弧内の数値は、装置が保持する鍵情報の数と、従来の装置が保持するラベルの数とを比較した場合の差分を示す。

[0148] また、装置1が保持する各鍵情報は、鍵情報項目D401にて示すように、部分集合520「1」とラベル521「A1」、部分集合522「134」とラベル523「A3RL」、部分集合

524「125678」とラベル525「A5RLRL」及び部分集合526「1345678」とラベル527「A5RLRRL」である。

(5)無効化装置特定部105

無効化された装置を識別する装置識別子を1個以上記憶する無効化装置記憶領域を有している。なお、無効化装置記憶領域は、初期状態では、何も記憶されていない。

[0149] 無効化装置特定部105は、受付部107より無効化する装置を登録する登録指示を受け取ると、続けて、無効化する装置の装置識別子を1以上受け取る。無効化装置特定部105は、受け取った1以上の装置識別子を、無効化装置記憶領域に記憶する。このとき、無効化装置特定部105は、これまでに記憶している装置識別子に続けて、受け取った1以上の装置識別子を記憶する。

[0150] 無効化装置特定部105は、受付部107より鍵無効化データの作成指示を受け取ると、受け取った作成指示を、鍵無効化データ生成部106へ出力する。

(6)鍵無効化データ生成部106

鍵無効化データ生成部106は、メディア鍵を予め記憶しているメディア鍵記憶領域を有している。

[0151] 鍵無効化データ生成部106は、共通鍵暗号アルゴリズム(例えば、DES)を有している。

鍵無効化データ生成部106は、無効化装置特定部105より作成指示を受け取ると、無効化装置特定部105の無効化装置記憶領域に、装置識別子が記憶されているか否かを判断、つまり無効化する装置の装置識別子(以下、無効な装置識別子という。)が無効化装置記憶領域に存在するか否かを判断する。

[0152] 無効な装置識別子が記憶されていないと判断する場合には、和集合により全装置の装置識別子を含むことのできる2つの部分集合と、それら部分集合に対応するデバイス鍵を、情報格納部102に格納されているデバイス鍵テーブルD100から読み出す。例えば、鍵無効化データ生成部106は、図5に示すデバイス鍵テーブルD100から、部分集合「1234567」とデバイス鍵「K8」とからなる組、及び部分集合「8」とデバイス鍵「K34」とからなる組を読み出す。なお、以降の説明において、読み出した

2つの部分集合を第1部分集合及び第2部分集合とし、それぞれに対応するデバイス鍵を第1デバイス鍵及び第2デバイス鍵とする。

- [0153] 鍵無効化データ生成部106は、メディア鍵をメディア鍵記憶領域から読み出し、読み出したメディア鍵を、第1デバイス鍵を用いて共通鍵暗号アルゴリズムで暗号化して、第1暗号化メディア鍵を生成し、生成した第1暗号化メディア鍵と、第1部分集合とを対応付けて一時的に記憶する。さらに、鍵無効化データ生成部106は、読み出したメディア鍵を、第2デバイス鍵を用いて共通鍵暗号アルゴリズムで暗号化して、第2暗号化メディア鍵を生成し、生成した第2暗号化メディア鍵と、第2部分集合とを対応付けて一時的に記憶する。
- [0154] 上記に示す例では、鍵無効化データ生成部106は、第1暗号化メディア鍵 $\text{Enc}(K8, \text{メディア鍵})$ 、及び第2暗号化メディア鍵 $\text{Enc}(K34, \text{メディア鍵})$ を生成し、それぞれ、部分集合「1234567」、及び部分集合「8」と対応付けて一時的に記憶する。ここで、 $\text{Enc}(A, B)$ は、暗号化アルゴリズムEを適用して、鍵Aを用いて、データBを暗号化することを示している。
- [0155] 無効な装置識別子が記憶されていると判断する場合には、鍵無効化データ生成部106は、木構造T100にて管理している全装置識別子から無効な装置識別子を除いた1以上の装置識別子(以下、有効な装置識別子という。)のうち、最も多くの有効な装置識別子からなる部分集合及びその部分集合に対応するデバイス鍵をデバイス鍵テーブルD100から読み出す。読み出した部分集合及びデバイス鍵を一時的に記憶する。この動作を、全ての有効な装置識別子のみが部分集合の要素として選択されるまで、繰り返し行う。鍵無効化データ生成部106は、この動作により、部分集合とその部分集合に対応するデバイス鍵とからなる1以上の組を、読み出した順に一時的に記憶する。
- [0156] 鍵無効化データ生成部106は、メディア鍵をメディア鍵記憶領域から読み出し、読み出したメディア鍵を、一時的に記憶している各デバイス鍵を用いて共通鍵暗号アルゴリズムで暗号化して、1個以上の暗号化メディア鍵を生成し、生成した各暗号化メディア鍵を、暗号化に利用したデバイス鍵に対応する部分集合と対応付けて一時的に記憶する。このとき、生成する暗号化メディア鍵の個数は、読み出したデバイス鍵

の個数と同じである。

- [0157] 例えば、無効化装置記憶領域に、装置識別子「1」が記憶されている場合には、鍵無効化データ生成部106は、部分集合「2345678」とデバイス鍵「K28」を読み出し、読み出したデバイス鍵を用いて、暗号化メディア鍵Enc(K28、メディア鍵)を生成し、生成した暗号化メディア鍵Enc(K28、メディア鍵)と部分集合「2345678」とを対応付けて一時的に記憶する。また、無効化装置記憶領域に、装置識別子「1」及び「5」が記憶されている場合には、鍵無効化データ生成部106は、部分集合「234」とデバイス鍵「K16」とからなる組、及び部分集合「678」とデバイス鍵「K33」とからなる組を読み出し、読み出したデバイス鍵「K16」及び「K33」を用いて、暗号化メディア鍵Enc(K16、メディア鍵)及びEnc(K33、メディア鍵)を生成し、生成した暗号化メディア鍵Enc(K16、メディア鍵)と部分集合「234」とを対応付け、暗号化メディア鍵Enc(K33、メディア鍵)と部分集合「678」とを対応付けて、それぞれ一時的に記憶する。
- [0158] 鍵無効化データ生成部106は、読み出したデバイス鍵全てから、暗号化メディア鍵の生成が終了すると、一時的に記憶している1以上の暗号化メディア鍵と部分集合との組(以下、鍵無効化データという。)を読み出し、読み出した1以上の鍵無効化データを、出力部108を介して記録媒体200aへ書き込む。鍵無効化データ生成部106は、次に、一時的に記憶している各情報を消去する。
- [0159] これにより、鍵無効化データ生成部106は、暗号化メディア鍵と部分集合との組からなる鍵無効化データを1以上生成し、生成した鍵無効化データを記録媒体200aへ記録することができる。

(7) 受付部107

受付部107は、ユーザの操作により、生成指示を受け付け、受け付けた生成指示を情報生成部103へ出力する。

- [0160] 受付部107は、ユーザの操作により、配布指示を受け付けると、続けて、配布する装置を示す装置識別子を受け付ける。受付部107は、受け付けた配布指示及び装置識別子を配布部104へ出力する。

受付部107は、ユーザの操作により、登録指示を受け付けると、続けて、無効化する装置の装置識別子を1以上受け付ける。受付部107は、受け付けた登録指示及び

1以上の装置識別子が無効化装置特定部105へ出力する。

- [0161] 受付部107は、ユーザの操作により、鍵無効化データの作成指示を受け取ると、受け取った作成指示を、無効化装置特定部105へ出力する。

(8)出力部108

出力部108は、鍵無効化データ生成部106から情報を受け取り、受け取った情報を書き込むための領域である鍵無効化データ格納部201を記録媒体200a上に確保し、受け取った情報を、確保した鍵無効化データ格納部201へ書き込む。

- [0162] 1. 3 記録媒体200

記録媒体200は、DVD-RAM等のレコーダブルメディアであって初期状態として何らの情報も記録されていない。

記録媒体200には、図13にて示すように、鍵管理装置100の鍵無効化データ生成部106の動作終了後において、鍵無効化データ格納部201が確保され、さらに、後述する記録装置300の動作により、暗号化コンテンツ鍵格納部202及び暗号化コンテンツ格納部203が確保される。

- [0163] (1)鍵無効化データ格納部201

鍵無効化データ格納部201は、鍵管理装置100の鍵無効化データ生成部106の動作により、何ら情報も記録されていない記録媒体200aから初めて確保される領域である。

鍵無効化データ格納部201には、暗号化メディア鍵と、各暗号化メディア鍵に対応付けられた部分集合とからなる組、つまり鍵無効化データが1以上記録される。

- [0164] なお、上述したように、鍵無効化データが1以上記録された記録媒体200を記録媒体200bを記述する。

(2)暗号化コンテンツ鍵格納部202及び暗号化コンテンツ格納部203

暗号化コンテンツ鍵格納部202及び暗号化コンテンツ格納部203は、記録装置300の動作により、記録媒体200bの状態から確保される領域である。

- [0165] 暗号化コンテンツ格納部203には、コンテンツを、コンテンツ鍵を用いて共通鍵暗号アルゴリズム(例えば、DES)で暗号化した暗号化コンテンツが記録される。

暗号化コンテンツ鍵格納部202には、コンテンツ鍵を、メディア鍵を用いて共通鍵

暗号アルゴリズム(例えば、DES)で暗号化した暗号化コンテンツ鍵が記録される。

1. 4 記録装置300

記録装置300a、300b、・・・、300cは、同様の構成を有しているため、ここでは、記録装置300として説明する。

[0166] 記録装置300は、図14に示すように、鍵情報格納部301、コンテンツ格納部302、コンテンツ鍵格納部303、復号鍵生成部304、復号部305、第1暗号化部306、第2暗号化部307、受付部308及び入出力部309から構成されている。

記録装置300は、具体的には、マイクロプロセッサ、ROM、RAM、ハードディスクユニットなどから構成されるコンピュータシステムである。前記RAM又は前記ハードディスクユニットには、コンピュータプログラムが記憶されている。前記マイクロプロセッサが、前記コンピュータプログラムに従って動作することにより、記録装置300は、その機能を達成する。

[0167] 記録装置300は、当該記録装置300を識別するための装置識別子を予め記憶している。

なお、以降の説明では、記録装置300に記録媒体200bが装着されているものとする。

(1) 鍵情報格納部301

鍵情報格納部301は、鍵管理装置100より配布された1以上の鍵情報と相互関係テーブルD101を予め記憶している。

[0168] 例えば、記録装置300が、装置識別子1を予め記憶している場合には、図12にて示す装置1が保持する4つの鍵情報を記憶し、装置識別子2を予め記憶している場合には、図12にて示す装置2が保持する5つの鍵情報を記憶している。

(2) コンテンツ格納部302

コンテンツ格納部302は、映像情報及び音声情報からなるコンテンツを予め記憶している。

[0169] (3) コンテンツ鍵格納部303

コンテンツ鍵格納部303は、コンテンツ格納部302にて記憶しているコンテンツを暗号化するためのコンテンツ鍵を記憶している。

(4) 復号鍵生成部304

復号鍵生成部304は、鍵管理装置100の情報生成部103が有する擬似乱数生成器G150と同一の擬似乱数生成器G151を予め記憶している。擬似乱数生成器G151は、擬似乱数生成器G150と同一であるため、ここでの説明は省略する。

[0170] 復号鍵生成部304は、受付部308より、暗号化コンテンツを記録媒体200bに記録する記録指示を受け取ると、入出力部309を介して当該記録装置300に装着された記録媒体200bより、記録媒体200bに記録されている1以上の暗号化メディア鍵のそれぞれに対応する部分集合のうち、1つの部分集合(以下、基準部分集合という。)を読み出す。

[0171] 復号鍵生成部304は、鍵情報格納部301から相互関係テーブルD101と1以上の鍵情報とを読み出す。

復号鍵生成部304は、相互関係テーブルD101を用いて、読み出した各鍵情報に含まれる部分集合から、基準部分集合に至る経路をもつ部分集合を検索する。

検索結果により、読み出した各鍵情報に含まれる各部分集合から、基準部分集合に至る経路をもつ部分集合(以下、検出部分集合という。)を検出した場合には、復号鍵生成部304は、以下に示すデバイス鍵の取得動作により、暗号化メディア鍵の復号鍵であるデバイス鍵を取得し、取得したデバイス鍵と、基準部分集合とを復号部305へ出力する。ここで、基準部分集合と一致する部分集合が、読み出した各鍵情報に含まれる各部分集合に含まれている場合には、復号鍵生成部304は、その一致する部分集合を検出部分集合として検出する。

[0172] 検索結果により、検出部分集合を検出しない場合には、未読出の基準部分集合が、記録媒体200bに1つ以上存在するか否かを判断し、存在すると判断する場合には、1以上の未読出の基準部分集合のうち1つの基準部分集合を読み出し、検出部分集合の検索を行う。未読出の基準部分集合が、記録媒体200bに存在しないと判断する場合には、暗号化コンテンツの記録の動作を終了する。

[0173] <デバイス鍵の取得動作>

復号鍵生成部304は、検出部分集合を含む鍵情報から、Xビットからなるラベルを取得する。

検出部分集合から基準部分集合までの経路に存在するノードの個数Zを取得する。復号鍵生成部304は、以下のようにして、擬似乱数生成器G151をZ回利用する。

[0174] 復号鍵生成部304は、取得したラベルを入力値として、擬似乱数生成器G151を用いて、3Xビットからなる乱数を生成して取得する。復号鍵生成部304は、検出部分集合から基準部分集合までに至る経路において、入力値として利用したラベルに対応する部分集合に対する次のノード(つまり、子ノード)が存在するか否かを判断する。存在すると判断する場合には、その次のノードが、左の子ノードであるか右の子ノードであるかを判断する。左の子ノードであると判断する場合には、取得した3Xビットの乱数をXビットごとに分割することにより、左ラベルを取得し、取得した左ラベルを擬似乱数生成器G151に対する次の入力値とし、右の子ノードであると判断する場合には、取得した3Xビットの乱数をXビットごとに分割することにより、右ラベルを取得し、取得した右ラベルを擬似乱数生成器G151に対する次の入力値とする。次のノードが存在しないと判断する場合、つまり、入力値として利用したラベルに対応する部分集合が基準部分集合である場合には、右ラベル及び左ラベルの取得は行わない。

[0175] 復号鍵生成部304は、擬似乱数生成器G151をZ回利用することにより、基準部分集合に対するラベルを入力値とした場合における擬似乱数生成器G151の出力値である、3Xビットからなる乱数を生成して取得することができる。

復号鍵生成部304は、Z回目に取得した3Xビットの乱数をXビットごとに分割し、左から2番目に位置するXビットを、暗号化メディア鍵の復号に用いるデバイス鍵として取得する。

[0176] (デバイス鍵の取得の具体例)

ここで、デバイス鍵の取得の具体例として、記録装置300が装置識別子1を有する場合、記録装置300が装置識別子2を有する場合、及び記録装置300が装置識別子3を有する場合について、説明する。このとき、記録媒体200bは、図15に示すように、鍵無効化データ格納部201に、部分集合「2345678」と暗号化メディア鍵(K28、メディア鍵)とを記憶している。

[0177] 記録装置300が、装置識別子1を有している場合には、記憶している4つの鍵情報のそれぞれに含まれる部分集合から基準部分集合「2345678」へ至る経路は存在し

ないため、復号鍵生成部304は、暗号化メディア鍵を復号するデバイス鍵を生成することはできない。

記録装置300が、装置識別子2を有している場合には、記憶している5つの鍵情報のそれぞれに含まれる部分集合から基準部分集合「2345678」へ至る経路をもつ部分集合として、部分集合「2345678」を検出し、検出した部分集合「2345678」を検出部分集合とする。復号鍵生成部304は、検出部分集合を含む鍵情報からラベル「A5RLRRR」を取得する。さらに、復号鍵生成部304は、検出部分集合から基準部分集合までに至るノード数 $Z=1$ を取得する。復号鍵生成部304は、取得したラベル「A5RLRRR」を入力値として、擬似乱数生成器G151を $Z=1$ 回利用して、3Xビットからなる乱数を生成し取得する。復号鍵生成部304は、取得した3Xビットの乱数をXビットごとに分割し、左から2番目に位置するXビットを、暗号化メディア鍵の復号に用いるデバイス鍵「K28」として取得する。

[0178] 記録装置300が、装置識別子3を有している場合には、記憶している4つの鍵情報のそれぞれに含まれる部分集合から基準部分集合「2345678」へ至る経路をもつ部分集合として、部分集合「345678」を検出し、検出した部分集合「345678」を検出部分集合とする。復号鍵生成部304は、検出部分集合を含む鍵情報からラベル「A5RLRR」を取得する。さらに、復号鍵生成部304は、検出部分集合から基準部分集合までに至るノード数 $Z=2$ を取得する。復号鍵生成部304は、以下のようにして擬似乱数生成器G151を $Z=2$ 回利用して、デバイス鍵「K28」を取得する。

[0179] 復号鍵生成部304は、先ず、取得したラベル「A5RLRR」を入力値として、擬似乱数生成器G151を利用して、3Xビットからなる乱数「A5RLRRL | | K24 | | A5RLRRR」を生成し取得する。入力値として利用したラベルに対応する部分集合「345678」に対する子ノードである部分集合「2345678」が左の子ノードであるか右の子ノードであるかを判断する。この場合、右の子ノードであると判断し、取得した右ラベル「A5RLRRR」を、擬似乱数生成器G151に対する次の入力値として取得する。復号鍵生成部304は、取得したラベル「A5RLRRR」を入力値として、擬似乱数生成器G151を利用して、3Xビットからなる乱数「A5RLRRRL | | K28 | | A5RLRRRR」を生成し取得する。復号鍵生成部304は、取得した3Xビットの乱数をXビットごとに

分割し、左から2番目に位置するXビットを、暗号化メディア鍵の復号に用いるデバイス鍵「K28」として取得する。

[0180] (5)復号部305

復号部305は、暗号化メディア鍵を生成した共通鍵暗号化アルゴリズムと同じ共通鍵暗号化アルゴリズムを有している。

復号部305は、復号鍵生成部304からデバイス鍵と、基準部分集合とを受け取ると、記録媒体200bの鍵無効化データ格納部201から、受け取った基準部分集合に対応する暗号化メディア鍵を、入出力部309を介して読み出す。

[0181] 復号部305は、読み出した暗号化メディア鍵を、受け取ったデバイス鍵を用いて共通鍵暗号アルゴリズムで復号して、メディア鍵を生成し、生成したメディア鍵を第1暗号化部306へ出力する。

(6)第1暗号化部306

第1暗号化部306は、共通鍵暗号アルゴリズム(例えば、DES)を有している。

[0182] 第1暗号化部306は、復号部305からメディア鍵を受け取ると、コンテンツ鍵格納部303よりコンテンツ鍵を読み出す。

第1暗号化部306は、読み出したコンテンツ鍵を、メディア鍵を用いて共通鍵暗号アルゴリズムで暗号化して、暗号化コンテンツ鍵Enc(メディア鍵、コンテンツ鍵)を生成し、生成した暗号化コンテンツ鍵を、入出力部309を介して記録媒体200bの暗号化コンテンツ鍵格納部202へ書き込む。

[0183] さらに、第1暗号化部306は、第2暗号化部307へコンテンツの暗号化を指示する旨の暗号化命令を出力する。

(7)第2暗号化部307

第2暗号化部307は、共通鍵暗号アルゴリズム(例えば、DES)を有している。

第2暗号化部307は、第1暗号化部306から、暗号化命令を受け取ると、コンテンツ鍵格納部303よりコンテンツ鍵を、コンテンツ格納部302からコンテンツを、それぞれ読み出す。

[0184] 第2暗号化部307は、読み出したコンテンツを、読み出したコンテンツ鍵を用いて共通鍵暗号アルゴリズムで暗号化して、暗号化コンテンツEnc(コンテンツ鍵、コンテン

ツ)を生成し、生成した暗号化コンテンツを、入出力部309を介して記録媒体200bの暗号化コンテンツ格納部203へ書き込む。

なお、第1暗号化部306及び第2暗号化部307が、各情報を記録媒体200bへ書き込むことにより、記録媒体200cが生成されていることに注意されたい。

[0185] (8)受付部308

受付部308は、ユーザの操作により、記録指示を受け付け、受け付けた記録指示を復号鍵生成部304へ出力する。

(9)入出力部309

入出力部309は、基準部分集合を、記録媒体200bの鍵無効化データ格納部201から読み出し、読み出した基準部分集合を復号鍵生成部304へ出力する。

[0186] 入出力部309は、基準部分集合に対応する暗号化メディア鍵を、記録媒体200bの鍵無効化データ格納部201から読み出し、読み出した暗号化メディア鍵を復号部305へ出力する。

入出力部309は、第1暗号化部306から暗号化コンテンツ鍵を受け取り、受け取った暗号化コンテンツ鍵を書き込むために、暗号化コンテンツ鍵格納部202を記録媒体200b上に確保し、確保した暗号化コンテンツ鍵格納部202に受け取った暗号化コンテンツ鍵を書き込む。

[0187] 入出力部309は、第2暗号化部307から暗号化コンテンツを受け取り、受け取った暗号化コンテンツを書き込むために、暗号化コンテンツ格納部203を記録媒体200b上に確保し、確保した暗号化コンテンツ格納部203に受け取った暗号化コンテンツを書き込む。

1. 5 再生装置400

再生装置400a、400b、・・・、400cは、同様の構成を有しているので、ここでは、再生装置400として説明する。

[0188] 再生装置400は、図16に示すように、鍵情報格納部401、復号鍵生成部402、第1復号部403、第2復号部404、第3復号部405、再生部406、受付部407及び読出部408から構成されている。

再生装置400は、具体的には、マイクロプロセッサ、ROM、RAM、ハードディスク

ユニットなどから構成されるコンピュータシステムである。前記RAM又は前記ハードディスクユニットには、コンピュータプログラムが記憶されている。前記マイクロプロセッサが、前記コンピュータプログラムに従って動作することにより、再生装置400は、その機能を達成する。

[0189] 再生装置400は、当該再生装置400を識別するための装置識別子を予め記憶している。

なお、以降の説明では、再生装置400に記録媒体200cが装着されているものとする。

(1) 鍵情報格納部401

鍵情報格納部401は、鍵管理装置100より配布された1以上の鍵情報と相互関係テーブルD101を予め記憶している。

[0190] 例えば、再生装置400が、装置識別子5を予め記憶している場合には、図12にて示す装置5が保持する4つの鍵情報を記憶し、装置識別子6を予め記憶している場合には、図12にて示す装置6が保持する5つの鍵情報を記憶している。

(2) 復号鍵生成部402

復号鍵生成部402は、鍵管理装置100の情報生成部103が有する擬似乱数生成器G150と同一の擬似乱数生成器G152を予め記憶している。擬似乱数生成器G152は、擬似乱数生成器G150と同一であるため、ここでの説明は省略する。

[0191] 復号鍵生成部402は、受付部308より、コンテンツの再生する再生指示を受け取ると、読出部408を介して当該再生装置400に装着された記録媒体200cより、記録媒体200cに記録されている1以上の暗号化メディア鍵のそれぞれに対応する部分集合のうち、1つの基準部分集合を読み出す。

復号鍵生成部402は、鍵情報格納部401から相互関係テーブルD101と1以上の鍵情報とを読み出す。

[0192] 復号鍵生成部304は、相互関係テーブルD101を用いて、読み出した各鍵情報に含まれる部分集合から、基準部分集合に至る経路をもつ検出部分集合を検索する。

検索結果により、読み出した各鍵情報に含まれる部分集合から、検出部分集合を検出した場合には、復号鍵生成部402は、デバイス鍵の取得動作により、暗号化メ

ディア鍵の復号鍵であるデバイス鍵を取得し、取得したデバイス鍵と、基準部分集合とを第1復号部403へ出力する。

[0193] 検索結果により、検出部分集合を検出しない場合には、未読出の基準部分集合が、記録媒体200cに1つ以上存在するか否かを判断し、存在すると判断する場合には、1以上の未読出の基準部分集合のうち1つの基準部分集合を読み出し、検出部分集合の検索を行う。未読出の基準部分集合が、記録媒体200cに存在しないと判断する場合には、コンテンツの再生の動作を終了する。

[0194] なお、デバイス鍵の取得動作は、記録装置300の復号鍵生成部304にて示す取得動作と同様であるため、説明は省略する。

<デバイス鍵の取得の具体例>

ここで、デバイス鍵の取得の具体例として、再生装置400が装置識別子1を有する場合、及び再生装置400が装置識別子7を有する場合について、説明する。このとき、記録媒体200cは、図17に示すように、鍵無効化データ格納部201に、部分集合「2345678」と暗号化メディア鍵(K28、メディア鍵)とを記憶し、暗号化コンテンツ鍵格納部202に、暗号化コンテンツ鍵Enc(メディア鍵、コンテンツ鍵)を記憶し、暗号化コンテンツ格納部203に、暗号化コンテンツEnc(コンテンツ鍵、コンテンツ)を記憶している。

[0195] 再生装置400が、装置識別子1を有している場合には、記憶している4つの鍵情報のそれぞれに含まれる部分集合から基準部分集合「2345678」へ至る経路は存在しないため、復号鍵生成部304は、暗号化メディア鍵を復号するデバイス鍵を生成することはできない。

再生装置400が、装置識別子7を有している場合には、記憶している5つの鍵情報のそれぞれに含まれる部分集合から検出部分集合「567」を検出し、検出部分集合を含む鍵情報からラベル「A5RL」を取得する。復号鍵生成部402は、擬似乱数生成器G152と、取得したラベル「A5RL」とを用いて、デバイス鍵「K28」を取得する。

[0196] (3)第1復号部403

第1復号部403は、暗号化メディア鍵を生成した共通鍵暗号化アルゴリズムと同じ共通鍵暗号化アルゴリズムを有している。

第1復号部403は、復号鍵生成部402からデバイス鍵と、基準部分集合とを受け取ると、記録媒体200cの鍵無効化データ格納部201から、受け取った基準部分集合に対応する暗号化メディア鍵を、読出部408を介して読み出す。

- [0197] 第1復号部403は、読み出した暗号化メディア鍵を、受け取ったデバイス鍵を用いて共通鍵暗号アルゴリズムで復号して、メディア鍵を生成し、生成したメディア鍵を第2復号部404へ出力する。

(4) 第2復号部404

第2復号部404は、暗号化コンテンツ鍵を生成した共通鍵暗号化アルゴリズムと同じ共通鍵暗号化アルゴリズムを有している。

- [0198] 第2復号部404は、第1復号部403からメディア鍵を受け取ると、読出部408を介して記録媒体200cの暗号化コンテンツ鍵格納部202から、暗号化コンテンツ鍵を読み出す。

第2復号部404は、読み出した暗号化コンテンツ鍵を、受け取ったメディア鍵を用いて共通鍵暗号アルゴリズムで復号して、コンテンツ鍵を生成し、生成したコンテンツ鍵を第3復号部405へ出力する。

- [0199] (5) 第3復号部405

第3復号部405は、暗号化コンテンツを生成した共通鍵暗号化アルゴリズムと同じ共通鍵暗号化アルゴリズムを有している。

第3復号部405は、第2復号部404からコンテンツ鍵を受け取ると、読出部408を介して記録媒体200cの暗号化コンテンツ格納部203から、暗号化コンテンツを読み出す。

- [0200] 第3復号部405は、読み出した暗号化コンテンツを、受け取ったコンテンツ鍵を用いて共通鍵暗号アルゴリズムで復号して、コンテンツを生成し、生成したコンテンツを再生部406へ出力する。

(6) 再生部406

再生部406は、第3復号部405からコンテンツDCNTを受け取り、受け取ったコンテンツから映像情報及び音声情報を生成し、生成した映像情報及び音声情報をアナログの映像信号及び音声信号に変換し、アナログの映像信号及び音声信号をモ

ニタ420へ出力する。

[0201] (7)受付部407

受付部407は、ユーザの操作により再生指示を受け付け、受け付けた再生指示を復号鍵生成部402へ出力する。

(8)読出部408

読出部408は、基準部分集合を、記録媒体200cの鍵無効化データ格納部201から読み出し、読み出した基準部分集合を復号鍵生成部402へ出力する。

[0202] 読出部408は、基準部分集合に対応する暗号化メディア鍵を、記録媒体200cの鍵無効化データ格納部201から読み出し、読み出した暗号化メディア鍵を第1復号部403へ出力する。

読出部408は、暗号化コンテンツ鍵を、記録媒体200cの暗号化コンテンツ鍵格納部202から読み出し、読み出した暗号化コンテンツ鍵を第2復号部404へ出力する。

[0203] 読出部408は、暗号化コンテンツを、記録媒体200cの暗号化コンテンツ格納部203から読み出し、読み出した暗号化コンテンツを第3復号部405へ出力する。

(9)モニタ420

モニタ420は、CRT及びスピーカを備え、再生部406からアナログの映像信号及び音声信号を受信し、映像信号に基づいて映像を表示し、音声信号に基づいて音声を出力する。

[0204] 1. 6 鍵管理装置100の動作

ここでは、鍵管理装置100が、生成指示を受け取ったときの動作、鍵情報の配布時の動作及び鍵無効化データの生成時の動作について動作について、説明する。

(1)生成処理の動作概要

ここでは、鍵管理装置100が生成指示を受け取ったときの動作の概要について、図18に示す流れ図を用いて、説明する。

[0205] 鍵管理装置100の情報生成部103は、受付部107より生成指示を受け取ると(ステップS5)、部分集合の生成処理を行い、1以上の部分集合が記録されているデバイス鍵テーブルD100aを生成する(ステップS10)。

情報生成部103は、次に、デバイス鍵の生成処理を行い、デバイス鍵テーブルD1

00及び相互関係テーブルD101を生成する(ステップS15)。

[0206] (2) 部分集合の生成処理の動作

ここでは、部分集合の生成処理の動作について、図19及び図20に示す流れ図を用いて、説明する。

情報生成部103は、装置情報格納部101にて管理している木構造の高さTを取得し(ステップS50)、作業用デバイス鍵テーブルの行カウンタnに初期値0をセットする(ステップS55)。

[0207] 情報生成部103は、 $i=0 \sim T-1$ までの間、ステップS65〜ステップS110を繰り返す。

情報生成部103は、レイヤiの存在するノードの数Nを取得する(ステップS65)。次に、情報生成部103は、レイヤiに存在するノードをルートとする部分木の高さHを取得する(ステップS70)。

[0208] 情報生成部103は、 $j=0 \sim H-1$ までの間、ステップS80〜ステップS105を繰り返す。

情報生成部103は、行カウンタnに1を加算し、加算結果をnとする(ステップS80)。

次に、情報生成部103は、 $k=1 \sim N$ までの間、ステップS90〜ステップS100を繰り返す。

[0209] 情報生成部103は、レイヤiの左からk番目のノードをルートとする部分木を取得し(ステップS90)、取得した部分木のリーフから、 2^j 個の端末識別子を除き、残りの端末識別子からなる部分集合を1個以上生成する(ステップS95)。ただし、複数の装置を除く場合、つまり複数の無効な装置識別子を除く場合には、無効な端末識別子全てが共通にもち、且つ無効な端末装置識別子だけがもつ上位ノードが存在する場合のみとする。

[0210] 情報生成部103は、生成した各部分集合を、作業用デバイス鍵テーブルのn行目の未記録の列に対して、左から順に書き込む(ステップS100)。

(3) デバイス鍵の生成処理の動作

ここでは、デバイス鍵の生成処理の動作について、図21〜図25に示す流れ図を用いて、説明する。

[0211] 情報生成部103は、装置情報格納部101にて管理している木構造の高さ T を取得する(ステップS150)。

情報生成部103は、 $h=1 \sim 2^T$ までの間、ステップS160〜ステップS345を繰り返す。

情報生成部103は、 X ビットからなる乱数 A_h を生成し(ステップS160)、生成した乱数 A_h を、デバイス鍵テーブルD100aの $\{(T^2+T)/2\}$ 行、 h 列へ書き込む(ステップS165)。

[0212] 情報生成部103は、擬似乱数生成器 G に、割り当てられたラベル、つまり乱数 A_h を入力値として与え、その出力としてデバイス鍵「 K_m 」、左ラベル及び右ラベルを取得する(ステップS170)。

情報生成部103は、取得したデバイス鍵「 K_m 」を、デバイス鍵テーブルD100aの $\{(T^2+T)/2\}$ 行、 h 列へ書き込む(ステップS175)。情報生成部103は、左ラベル及び右ラベルを、擬似乱数生成器 G への入力に使用したラベル(つまり、乱数 A_h)に対する部分集合と対応付けて、一時的に記憶しておく(ステップS180)。ただし、デバイス鍵を示す「 K_m 」の添字 m は、初期値1から始まり、デバイス鍵が割り当てられる毎に1ずつ増加する値とし、「 K_{m+1} 」は、「 K_m 」の次に割り当てられるデバイス鍵であることを示す。

[0213] 情報生成部103は、 $i=\{(T^2+T)/2-1\} \sim 1$ までの間、ステップS190〜ステップS340を繰り返す。

情報生成部103は、デバイス鍵テーブルD100aの $i+1$ 行目でデバイス鍵が割り当てられた部分集合の個数 J を取得する(ステップS190)。

情報生成部103は、 $j=1 \sim J$ までの間、ステップS200〜ステップS335を繰り返す。

[0214] 情報生成部103は、デバイス鍵テーブルD100aの $i+1$ 行目でデバイス鍵が割り当てられた左から j 番目の部分集合 S_j を基準として、デバイス鍵テーブルD100aの i 行目を左から順に、部分集合 S_j を含み、且つデバイス鍵が未だ割り当てられていない部分集合を検索する(ステップS200)。

情報生成部103は、検索により、部分集合 S_j を含み、デバイス鍵が未だ割り当てられていない部分集合が存在するか否かを判断する(ステップS205)。

[0215] 部分集合が存在しないと判断する場合には(ステップS205における「NO」)、部分集合 S_j を親ノードとし、親ノードである部分集合 S_j と、その子ノードとなる部分集合が存在しないことを示す記号「-」とからなる組を、ノード情報として、作業用相互関係テーブル内の未記録である最上位の領域へ書き込む(ステップS210)。さらに、部分集合 S_j がルートであるか否かを判断し(ステップS215)、ルートであると判断する場合には(ステップS215における「YES」)、ルート情報に、ルートであることを示す情報(「ルート」)を記録する(ステップS220)。ルートでないと判断する場合には(ステップS215における「NO」)、ステップS220を省略する。

[0216] 部分集合が1以上存在すると判断する場合には(ステップS205における「YES」)、デバイス鍵が未だ割り当てられていない1以上の部分集合のうち最大2つの部分集合を左から順に取得する(ステップS225)。

情報生成部103は、取得した部分集合が1つであるか否かを判断する(ステップS230)。

[0217] 取得した部分集合が1つであると判断する場合には(ステップS230における「YES」)、部分集合 S_j に対応付けられ、一時的に記憶している左ラベル及び右ラベルのうち右ラベルを、取得した部分集合に対するラベルとして割り当て、割り当てた右ラベルを、デバイス鍵テーブルD100a内の取得した部分集合が記録されている欄へ書き込む(ステップS235)。

[0218] 情報生成部103は、擬似乱数生成器Gに、取得した部分集合に割り当てられたラベル(つまり、一時的に記憶している右ラベル)を入力値として与え、その出力としてデバイス鍵「 K_m 」、左ラベル及び右ラベルを取得する(ステップS240)。

情報生成部103は、取得したデバイス鍵「 K_m 」を、デバイス鍵テーブルD100a内の取得した部分集合が記録されている欄へ書き込む(ステップS245)。さらに、情報生成部103は、ステップS240にて取得した2つの左ラベル及び右ラベルを、擬似乱数生成器Gへの入力に使用したラベルに対する部分集合(つまり、ステップS225にて取得した部分集合)と対応付けて、一時的に記憶しておく(ステップS250)。情報生成部103は、部分集合 S_j を親ノードとし、取得した部分集合をその子ノードとして、作業用相互関係テーブル内の未記録である最上位の領域へ書き込む(ステップS255)。

)。さらに、部分集合 S_j がルートであるか否かを判断し(ステップS260)、ルートであると判断する場合には(ステップS260における「YES」)、ルート情報に、ルートであることを示す情報(「ルート」)を記録する(ステップS265)。ルートでないと判断する場合には(ステップS260における「NO」)、ステップS265を省略する。

[0219] 取得した部分集合が2つ(ここでは、 T_j 及び U_j とする)であると判断する場合には(ステップS230における「NO」)、2つの部分集合のうち左側に位置する部分集合 T_j に対するラベルとして、部分集合 S_j に対応付けられ、一時的に記憶している左ラベルを割り当て、割り当てた左ラベルをデバイス鍵テーブルD100a内の取得した部分集合 T_j が記録している欄へ書き込む(ステップS270)。

[0220] 情報生成部103は、擬似乱数生成器Gに、取得した部分集合 T_j に割り当てられたラベル(つまり、部分集合 S_j に対応する左ラベル)を入力値として与え、その出力としてデバイス鍵「 K_m 」、左ラベル及び右ラベルを取得する(ステップS275)。

情報生成部103は、取得したデバイス鍵「 K_m 」を、デバイス鍵テーブルD100a内の取得した部分集合が記録している欄へ書き込む(ステップS280)。さらに、情報生成部103は、ステップS275にて取得した2つの左ラベル及び右ラベルを、擬似乱数生成器Gへの入力に使用したラベルに対する部分集合 T_j と対応付けて、一時的に記憶しておく(ステップS285)。情報生成部103は、部分集合 S_j を親ノードとし、取得した部分集合 T_j をその子ノードとして、作業用相互関係テーブル内の未記録である最上位の領域へ書き込む(ステップS290)。さらに、部分集合 S_j がルートであるか否かを判断し(ステップS295)、ルートであると判断する場合には(ステップS295における「YES」)、ルート情報に、ルートであることを示す情報(「ルート」)を記録する(ステップS300)。ルートでないと判断する場合には(ステップS295における「NO」)、ステップS300を省略する。

[0221] 次に、情報生成部103は、部分集合 U_j に対するラベルとして、部分集合 S_j に対応付けられ、一時的に記憶している右ラベルを割り当て、割り当てた右ラベルをデバイス鍵テーブルD100a内の取得した部分集合 U_j が記録している欄へ書き込む(ステップS305)。

情報生成部103は、擬似乱数生成器Gに、取得した部分集合 U_j に割り当てられた

ラベル(つまり、部分集合 S_j に対応する右ラベル)を入力値として与え、その出力としてデバイス鍵「 K_{m+1} 」、左ラベル及び右ラベルを取得する(ステップS310)。

- [0222] 情報生成部103は、取得したデバイス鍵「 K_{m+1} 」を、デバイス鍵テーブルD100a内の取得した部分集合が記録されている欄へ書き込む(ステップS315)。さらに、情報生成部103は、ステップS310にて取得した2つの左ラベル及び右ラベルを、擬似乱数生成器Gへの入力に使用したラベルに対する部分集合 U_j と対応付けて、一時的に記憶しておく(ステップS320)。情報生成部103は、部分集合 S_j を親ノードとし、取得した部分集合 U_j をその子ノードとして、作業用相互関係テーブル内の未記録である最上位の領域へ書き込む(ステップS325)。さらに、部分集合 S_j がルートであるか否かを判断し(ステップS330)、ルートであると判断する場合には(ステップS330における「YES」)、ルート情報に、ルートであることを示す情報(「ルート」)を記録する(ステップS335)。ルートでないと判断する場合には(ステップS330における「NO」)、ステップS335を省略する。

- [0223] 情報生成部103は、生成したデバイス鍵テーブルD100及び相互関係テーブルD101を情報格納部102へ格納する(ステップS360)。

(4) 鍵情報の配布時の動作

ここでは、鍵情報の配布時に行う鍵情報の取得処理の動作について、図26及び図27に示す流れ図を用いて、説明する。

- [0224] 配布部104は、受付部107より、鍵情報の配布指示及び配布する装置を示す装置識別子とを受け取ると(ステップS400)、相互関係テーブルD101にて管理されている木構造の個数 Y を取得する(ステップS405)。

配布部104は、 $i=1$ 〜 Y までの間、ステップS415〜ステップS465を繰り返す。

- [0225] 配布部104は、相互関係テーブルD101にて上位から i 番目に管理されている木構造 V_i を示すデータ構造を取得する(ステップS415)。

配布部104は、取得したデータ構造から、子ノードを持たないノード(つまり、リーフ)の数 P を取得する(ステップS420)。

配布部104は、 $p=1$ 〜 P までの間、ステップS430〜ステップS460を繰り返す。

- [0226] 配布部104は、取得したデータ構造の親ノードの項目から、子ノードを持たない、

上位p番目のノードWp(つまり、Wpはリーフとなる。)を取得し(ステップS430)、木構造Viのルートを起点として、リーフWpまでに至る経路に対して、受け取った装置識別子を含む部分集合が出現する最初のノード(部分集合)を検索する(ステップS435)

。

[0227] 配布部104は、検索により、部分集合を検出したか否かを判断する(ステップS440)。

部分集合を検出したと判断する場合には(ステップS440における「YES」)、検出した部分集合が鍵情報記憶領域に記憶済みであるか否かを判断する(ステップS445)

。

[0228] 記憶済みでないと判断する場合には(ステップS445における「NO」)、配布部104は、検出した部分集合に対応するラベルをデバイス鍵テーブルD100から読み出し(ステップS450)、読み出したラベルと検出した部分集合とを含む鍵情報を生成して取得し(ステップS455)、取得した鍵情報を鍵情報記憶領域へ記憶する(ステップS460)。記憶済みであると判断する場合には(ステップS445における「YES」)、ステップS450ーステップS460を省略する。

[0229] 配布部104は、相互関係テーブルD101を読み出し(ステップS475)、読み出した相互関係テーブルD101と鍵情報記憶領域にて記憶している全ての鍵情報とを、配布対象の装置へ配布する(ステップS480)。

配布部104は、相互関係テーブルD101と全ての鍵情報とを、受け取った装置識別子をもつ装置へ配布した後、鍵情報記憶領域にて記憶している全ての鍵情報を消去する(ステップS485)。なお、ここで、配布とは、例えば、配布用の記録媒体に、受け付けた装置識別子と、鍵情報記憶領域にて記憶している1以上の鍵情報との書き込みが完了したことをいう。

[0230] (5) 鍵無効化データの生成時の動作

ここでは、鍵無効化データの生成時に行う鍵無効化データ生成処理の動作について、図28に示す流れ図を用いて、説明する。

鍵無効化データ生成部106は、無効化装置特定部105を介して受付部107より作成指示を受け取ると(ステップS500)、無効化装置特定部105の無効化装置記憶領

域に、装置識別子が記憶されているか否かを判断、つまり無効な装置識別子が無効化装置記憶領域に存在するか否かを判断する(ステップS505)。

- [0231] 無効な装置識別子が記憶されていないと判断する場合には(ステップS505における「NO」)、和集合により全装置の装置識別子を含むことのできる第1及び第2部分集合をデバイス鍵テーブルD100から読み出す(ステップS510)。

鍵無効化データ生成部106は、読み出した各部分集合に対応する第1及び第2デバイス鍵を、デバイス鍵テーブルD100から読み出す(ステップS515)。

- [0232] 鍵無効化データ生成部106は、メディア鍵をメディア鍵記憶領域から読み出し(ステップS520)、読み出したメディア鍵を、第1デバイス鍵を用いて共通鍵暗号アルゴリズムで暗号化して、第1暗号化メディア鍵を生成し、生成した第1暗号化メディア鍵と、第1部分集合とを対応付けて一時的に記憶する。さらに、鍵無効化データ生成部106は、読み出したメディア鍵を、第2デバイス鍵を用いて共通鍵暗号アルゴリズムで暗号化して、第2暗号化メディア鍵を生成し、生成した第2暗号化メディア鍵と、第2部分集合とを対応付けて一時的に記憶する(ステップS525)。

- [0233] 第1部分集合及び第1暗号化メディア鍵を、出力部108を介して記録媒体200aへ書き込む(ステップS530)。

第2部分集合及び第2暗号化メディア鍵を、出力部108を介して記録媒体200aへ書き込む(ステップS535)。

無効な装置識別子が記憶されていると判断する場合には(ステップS505における「YES」)、鍵無効化データ生成部106は、木構造T100にて管理している全装置識別子から無効な装置識別子を除いた1以上の有効な装置識別子のうち、最も多くの有効な装置識別子からなる部分集合をデバイス鍵テーブルD100から読み出す(ステップS540)。

- [0234] 読み出した部分集合に対応するデバイス鍵をデバイス鍵テーブルD100から読み出し(ステップS545)、読み出した部分集合及びデバイス鍵を一時的に記憶する(ステップS550)。鍵無効化データ生成部106は、全ての有効な装置識別子のみが部分集合の要素として選択されたか否かを判断する(ステップS555)。

選択されていないと判断する場合には(ステップS555における「NO」)、1以上の

未選択の有効な装置識別子を用いて、ステップS54以降を、再度実行する。

[0235] 選択されたと判断する場合には(ステップS555における「YES」)、鍵無効化データ生成部106は、メディア鍵をメディア鍵記憶領域から読み出し(ステップS560)、読み出したメディア鍵を、一時的に記憶している各デバイス鍵を用いて共通鍵暗号アルゴリズムで暗号化して、1個以上の暗号化メディア鍵を生成し、生成した各暗号化メディア鍵を、暗号化に利用したデバイス鍵に対応する部分集合と対応付けて一時的に記憶する(ステップS565)。このとき、生成する暗号化メディア鍵の個数は、読み出したデバイス鍵の個数と同じである。

[0236] 鍵無効化データ生成部106は、読み出したデバイス鍵全てから、暗号化メディア鍵の生成が終了すると、一時的に記憶している1以上の暗号化メディア鍵と部分集合との組を読み出し、読み出した1以上の組を、出力部108を介して記録媒体200aへ書き込む(ステップS570)。

1. 7 記録装置300の動作

ここでは、記録装置300が、記録指示を受け取ったときの動作について動作について、説明する。

[0237] (1)記録処理の動作

ここでは、記録装置300が記録指示を受け取ったときに、復号鍵生成部304、復号部305、第1暗号化部306及び第2暗号化部307にて行う記録処理の動作について、図29に示す流れ図を用いて、説明する。

記録装置300の復号鍵生成部304は、受付部308より、記録指示を受け取ると(ステップS600)、入出力部309を介して当該記録装置300に装着された記録媒体200bより、記録媒体200bに記録されている1以上の暗号化メディア鍵のそれぞれに対応する部分集合のうち、1つの部分集合(以下、基準部分集合という。)を読み出す(ステップS605)。

[0238] 復号鍵生成部304は、鍵情報格納部301から相互関係テーブルD101と1以上の鍵情報とを読み出す(ステップS610)。

復号鍵生成部304は、相互関係テーブルD101を用いて、読み出した各鍵情報に含まれる部分集合から、検出部分集合を検索する(ステップS615)。

検索結果により、読み出した各鍵情報に含まれる部分集合から、検出部分集合を検出したか否かを判断する(ステップS620)。

[0239] 検出しないと判断する場合には(ステップS620における「NO」)、未読出の基準部分集合が、記録媒体200bに1つ以上存在するか否かを判断する(ステップS625)。存在すると判断する場合には(ステップS625における「YES」)、1以上の未読出の基準部分集合のうち1つの基準部分集合を読み出し(ステップS630)、ステップS615へ戻る。未読出の基準部分集合が、記録媒体200bに存在しないと判断する場合には(ステップS625における「NO」)、暗号化コンテンツの記録の動作を終了する。

[0240] 検出部分集合を検出したと判断する場合には(ステップS620における「YES」)、デバイス鍵の取得処理を行い、デバイス鍵を取得する(ステップS635)。

次に、復号部305は、デバイス鍵取得処理にて取得されたデバイス鍵を用いて、復号処理を行い、暗号化メディア鍵を復号して、メディア鍵を生成する(ステップS640)。

[0241] 第1暗号化部306は、復号処理にて生成されたメディア鍵を用いて、第1暗号化処理を行い、暗号化コンテンツ鍵を生成する(ステップS645)。

第2暗号化部307は、コンテンツ鍵を用いて、第2暗号化処理を行い、暗号化コンテンツを生成する(ステップS650)。

(2) デバイス鍵の取得処理の動作

ここでは、図29に示す記録処理のステップS635にて行われるデバイス鍵の取得処理の動作について、図30に示す流れ図を用いて、説明する。

[0242] 復号鍵生成部304は、検出部分集合を含む鍵情報から、Xビットからなるラベルを取得する(ステップS700)。

検出部分集合から基準部分集合までの経路に存在するノードの個数Zを取得する(ステップS705)。

復号鍵生成部304は、 $z=1$ 〜Zまでの間、ステップS715〜ステップS735までを、繰り返す。

[0243] 復号鍵生成部304は、取得したラベルを入力値として、擬似乱数生成器G151を用いて、3Xビットからなる乱数を生成して取得する(ステップS715)。

復号鍵生成部304は、検出部分集合から基準部分集合までに至る経路において、入力値として利用したラベルに対応する部分集合に対する次のノードが存在するかどうかを判断する(ステップS720)。

[0244] 存在すると判断する場合には(ステップS720における「YES」)、次のノードが、左の子ノードであるか右の子ノードであるかを判断する(ステップS725)。左の子ノードであると判断する場合には(ステップS725における「YES」)、取得した3Xビットの乱数をXビットごとに分割することにより、左ラベルを取得し(ステップS730)、取得した左ラベルを擬似乱数生成器G151に対する次の入力値として、ステップS715へ戻る。右の子ノードであると判断する場合には(ステップS725における「NO」)、取得した3Xビットの乱数をXビットごとに分割することにより、右ラベルを取得し(ステップS735)、取得した右ラベルを擬似乱数生成器G151に対する次の入力値として、ステップS715へ戻る。

[0245] 次のノードが存在しないと判断する場合には(ステップS720における「NO」)、ステップS725〜ステップS735を省略する。

復号鍵生成部304は、Z回目に取得した3Xビットの乱数をXビットごとに分割し、左から2番目に位置するXビットを、暗号化メディア鍵の復号に用いるデバイス鍵として取得する(ステップS745)。

[0246] 復号鍵生成部304は、取得したデバイス鍵と、基準部分集合とを復号部305へ出力する(ステップS750)。

(3)復号処理の動作

ここでは、図29に示す記録処理のステップS640にて行われる復号処理の動作について、図31に示す流れ図を用いて、説明する。

[0247] 復号部305は、復号鍵生成部304からデバイス鍵と、基準部分集合とを受け取ると(ステップS800)、記録媒体200bの鍵無効化データ格納部201から、受け取った基準部分集合に対応する暗号化メディア鍵を、入出力部309を介して読み出す(ステップS805)。

復号部305は、読み出した暗号化メディア鍵を、受け取ったデバイス鍵を用いて共通鍵暗号アルゴリズムで復号して、メディア鍵を生成し(ステップS810)、生成したメ

ディア鍵を第1暗号化部306へ出力する(ステップS815)。

[0248] (4) 第1暗号化処理の動作

ここでは、図29に示す記録処理のステップS645にて行われる第1暗号化処理の動作について、図32に示す流れ図を用いて、説明する。

第1暗号化部306は、復号部305からメディア鍵を受け取ると(ステップS830)、コンテンツ鍵格納部303よりコンテンツ鍵を読み出す(ステップS835)。

[0249] 第1暗号化部306は、読み出したコンテンツ鍵を、メディア鍵を用いて共通鍵暗号アルゴリズムで暗号化して、暗号化コンテンツ鍵を生成し(ステップS840)、生成した暗号化コンテンツ鍵を、入出力部309を介して記録媒体200bの暗号化コンテンツ鍵格納部202へ書き込む(ステップS845)。

さらに、第1暗号化部306は、第2暗号化部307へコンテンツの暗号化を指示する旨の暗号化命令を出力する(ステップS850)。

[0250] (5) 第2暗号化処理の動作

ここでは、図29に示す記録処理のステップS650にて行われる第2暗号化処理の動作について、図33に示す流れ図を用いて、説明する。

第2暗号化部307は、第1暗号化部306から、暗号化命令を受け取ると(ステップS870)、コンテンツ鍵格納部303よりコンテンツ鍵を、コンテンツ格納部302からコンテンツを、それぞれ読み出す(ステップS875)。

[0251] 第2暗号化部307は、読み出したコンテンツを、読み出したコンテンツ鍵を用いて共通鍵暗号アルゴリズムで暗号化して、暗号化コンテンツを生成し(ステップS880)、生成した暗号化コンテンツを、入出力部309を介して記録媒体200bの暗号化コンテンツ格納部203へ書き込む(ステップS885)。

1. 8 再生装置400の動作

ここでは、再生装置400が、再生指示を受け取ったときの動作について動作について、説明する。

[0252] (1) 再生処理の動作

ここでは、再生装置400が再生指示を受け取ったときに、復号鍵生成部402、第1復号部403、第2復号部404、第3復号部405及び再生部406にて行う再生処理の

動作について、図34に示す流れ図を用いて、説明する。

再生装置400の復号鍵生成部402は、受付部407より、再生指示を受け取ると(ステップS900)、読出部408を介して当該再生装置400に装着された記録媒体200cより、記録媒体200cに記録されている1以上の暗号化メディア鍵のそれぞれに対応する部分集合のうち、1つの部分集合(以下、基準部分集合という。)を読み出す(ステップS905)。

[0253] 復号鍵生成部402は、鍵情報格納部401から相互関係テーブルD101と1以上の鍵情報とを読み出す(ステップS910)。

復号鍵生成部402は、相互関係テーブルD101を用いて、読み出した各鍵情報に含まれる部分集合から、検出部分集合を検索する(ステップS915)。

検索結果により、読み出した各鍵情報に含まれる部分集合から、検出部分集合を検出したか否かを判断する(ステップS920)。

[0254] 検出しないと判断する場合には(ステップS920における「NO」)、未読出の基準部分集合が、記録媒体200cに1つ以上存在するか否かを判断する(ステップS925)。存在すると判断する場合には(ステップS925における「YES」)、1以上の未読出の基準部分集合のうち1つの基準部分集合を読み出し(ステップS930)、ステップS915へ戻る。未読出の基準部分集合が、記録媒体200cに存在しないと判断する場合には(ステップS925における「NO」)、コンテンツ再生の動作を終了する。

[0255] 検出部分集合を検出したと判断する場合には(ステップS920における「YES」)、デバイス鍵の取得処理を行い、デバイス鍵を取得する(ステップS935)。

次に、第1復号部403は、デバイス鍵取得処理にて取得されたデバイス鍵を用いて、復号処理を行い、暗号化メディア鍵を復号して、メディア鍵を生成する(ステップS940)。

[0256] 第2復号部404は、第1復号処理にて生成されたメディア鍵を用いて、第2復号処理を行い、暗号化コンテンツ鍵を復号して、コンテンツ鍵を生成する(ステップS945)。

第3復号部405は、第2復号処理にて生成されたコンテンツ鍵を用いて、第2暗号化処理を行い、暗号化コンテンツを復号してコンテンツを生成する(ステップS950)。

[0257] 再生部406は、第3復号処理にて生成されたコンテンツを、再生する(ステップS955)。

(2) デバイス鍵の取得処理の動作

ここでは、図34に示す再生処理のステップS935にて行われるデバイス鍵の取得処理の動作について、図35に示す流れ図を用いて、説明する。

[0258] 復号鍵生成部402は、検出部分集合を含む鍵情報から、Xビットからなるラベルを取得する(ステップS1000)。

復号鍵生成部402は、検出部分集合から基準部分集合までの経路に存在するノードの個数Zを取得する(ステップS1005)。

復号鍵生成部402は、 $z=1$ 〜Zまでの間、ステップS1015〜ステップS1035までを繰り返す。

[0259] 復号鍵生成部402は、取得したラベルを入力値として、擬似乱数生成器G151を用いて、3Xビットからなる乱数を生成して取得する(ステップS1015)。

復号鍵生成部402は、検出部分集合から基準部分集合までに至る経路において、入力値として利用したラベルに対応する部分集合に対する次のノードが存在するかどうかを判断する(ステップS1020)。

[0260] 存在すると判断する場合には(ステップS1020における「YES」)、次のノードが、左の子ノードであるか右の子ノードであるかを判断する(ステップS1025)。左の子ノードであると判断する場合には(ステップS1025における「YES」)、取得した3Xビットの乱数をXビットごとに分割することにより、左ラベルを取得し(ステップS1030)、取得した左ラベルを擬似乱数生成器G151に対する次の入力値として、ステップS1015へ戻る。右の子ノードであると判断する場合には(ステップS1025における「NO」)、取得した3Xビットの乱数をXビットごとに分割することにより、右ラベルを取得し(ステップS1035)、取得した右ラベルを擬似乱数生成器G151に対する次の入力値として、ステップS1015へ戻る。

[0261] 次のノードが存在しないと判断する場合には(ステップS1020における「NO」)、ステップS1025〜ステップS1035を省略する。

復号鍵生成部402は、Z回目に取得した3Xビットの乱数をXビットごとに分割し、左

から2番目に位置するXビットを、暗号化メディア鍵の復号に用いるデバイス鍵として取得する(ステップS1045)。

[0262] 復号鍵生成部402は、取得したデバイス鍵と、基準部分集合とを第1復号部403へ出力する(ステップS1050)。

(3)第1復号処理の動作

ここでは、図34に示す再生処理のステップS940にて行われる復号処理の動作について、図36に示す流れ図を用いて、説明する。

[0263] 第1復号部403は、復号鍵生成部402からデバイス鍵と、基準部分集合とを受け取ると(ステップS1100)、記録媒体200cの鍵無効化データ格納部201から、受け取った基準部分集合に対応する暗号化メディア鍵を、読出部408を介して読み出す(ステップS1105)。

第1復号部403は、読み出した暗号化メディア鍵を、受け取ったデバイス鍵を用いて共通鍵暗号アルゴリズムで復号して、メディア鍵を生成し(ステップS1110)、生成したメディア鍵を第2復号部404へ出力する(ステップS1115)。

[0264] (4)第2復号処理の動作

ここでは、図34に示す再生処理のステップS945にて行われる第2復号処理の動作について、図37に示す流れ図を用いて、説明する。

第2復号部404は、第1復号部403からメディア鍵を受け取ると(ステップS1130)、読出部408を介して記録媒体200cの暗号化コンテンツ鍵格納部202から、暗号化コンテンツ鍵を読み出す(ステップS1135)。

[0265] 第2復号部404は、読み出した暗号化コンテンツ鍵を、受け取ったメディア鍵を用いて共通鍵暗号アルゴリズムで復号して、コンテンツ鍵を生成し(ステップS1140)、生成したコンテンツ鍵を第3復号部405へ出力する(ステップS1145)。

(4)第3復号処理の動作

ここでは、図34に示す再生処理のステップS950にて行われる第3復号処理の動作について、図38に示す流れ図を用いて、説明する。

[0266] 第3復号部405は、第2復号部404からコンテンツ鍵を受け取ると(ステップS1070)、読出部408を介して記録媒体200cの暗号化コンテンツ格納部203から、暗号化

コンテンツを読み出す(ステップS1075)。

第3復号部405は、読み出した暗号化コンテンツを、受け取ったコンテンツ鍵を用いて共通鍵暗号アルゴリズムで復号して、コンテンツを生成し(ステップS1080)、生成したコンテンツを再生部406へ出力する(ステップS1085)。

[0267] 1. 9 その他の変形例

本発明を上記の実施の形態に基づいて説明してきたが、本発明は、上記の実施の形態に限定されないのはもちろんである。以下のような場合も本発明に含まれる。

(1)本発明では、記録媒体200をDVD-RAMのようなレコーダブルメディアとする構成としたが、本発明はその構成に限定されるものではない。例えば、記録媒体をDVD-Videoのようなプリレコーディッドメディアとして、各再生装置がデバイス鍵を保有して、記録媒体に記録されたコンテンツを再生する構成であってもよい。また、この場合、記録装置は、デバイス鍵を生成するための鍵情報を保有する必要はなく、鍵管理装置から直接メディア鍵を受け取り、そのメディア鍵に基づいてコンテンツを暗号化して書き込む構成であってもよい。

[0268] (2)本発明では、コンテンツを暗号化するメカニズムとして、メディア鍵でコンテンツ鍵を暗号化して、コンテンツ鍵でコンテンツを暗号化する構成としたが、本発明はその構成に限定されるものではない。例えば、メディア鍵で直接コンテンツを暗号化して鍵階層を1つ減らす構成でもよく、逆にディスク鍵を導入して、メディア鍵でディスク鍵を暗号化して、ディスク鍵でコンテンツ鍵を暗号化して、コンテンツ鍵でコンテンツを暗号化して鍵階層を1つ増やす構成であってもよい。あるいは、鍵階層の途中で別途異なる情報を追加して鍵を変調するような構成であってもよい。

[0269] (3)本発明では、鍵無効化データと暗号化コンテンツを同一の記録媒体200に記録する構成としたが、本発明はその構成に限定されるものではない。例えば、鍵無効化データを記録する記録媒体と、暗号化コンテンツを記録する記録媒体を変えて配布する構成であってもよい。その場合、記録装置300、あるいは再生装置400では、まず、鍵無効化データが記録された記録媒体を挿入してメディア鍵を算出してから、別の記録媒体を挿入して、コンテンツの記録、あるいは再生を行う構成となる。

[0270] (4)本発明では、鍵無効化データを記録媒体200に記録して配布する構成として

が、本発明はその構成に限定されるものではない。例えば、インターネットなどの通信媒体を利用して、鍵無効化データを配布し、記録装置300及び再生装置400は、配布された鍵無効化データを記憶し、各装置は、暗号化メディア鍵を復号する際に、記憶している鍵無効化データを用いて復号する構成であってもよい。

[0271] または、各装置は、暗号化メディア鍵の復号を行う度に、通信媒体を利用して、鍵無効化データを受け取ってもよい。

また、本発明では、記録装置300は、生成した暗号化コンテンツ鍵及び暗号化コンテンツを、装着された記録媒体200へ書き込んだが、これに限定されない。例えば、記録装置300は、生成した暗号化コンテンツ鍵及び暗号化コンテンツを、通信媒体を介して、ネットワーク上のサーバが有する記録媒体へ記録するようにしてもよい。

[0272] (5) 本発明では、鍵無効化データ、並びに暗号化コンテンツを記録媒体200に記録して配布する構成としてが、本発明はその構成に限定されるものではない。例えば、放送や、インターネットなどの通信媒体を利用して配布する構成であってもよい。

(6) 本発明では、鍵管理装置100が各装置を管理するための木構造を2分木として構成したが、本発明はその構成に限定されるものではない。各装置を管理する木構造は n 分木(n は整数)であればよい。例えば、木構造は3分木であっても、4分木であってもよい。

[0273] また、鍵管理装置100が、鍵を管理、つまり部分集合の相互関係を管理するための木構造を2分木として構成したが、本発明はその構成に限定されるものではない。上記と同様に、部分集合の相互関係を管理する木構造は n 分木(n は整数)であればよい。

(7) 上記実施の形態において、鍵管理装置100は、異なる2つの入力値に対して異なる2つの値を出力する擬似乱数生成器Gを利用して、部分集合の関連付けを行ったが、これに限定されない。

[0274] 鍵管理装置100は、異なる2つの入力値に対して、同一の値を出力する擬似乱数生成器G__1を利用して、部分集合の関連付けを行ってもよい。

例えば、上記の実施の形態では、部分集合「1」と部分集合「12」とを関連付けしたが、擬似乱数生成器G__1を利用することにより、部分集合「12」は、部分集合「1」及

び部分集合「2」のそれぞれと関連付けが可能となる。これにより、装置識別子「2」を有する装置は、部分集合「12」を含む鍵情報を保持する必要がなくなり、保持する鍵情報の個数を削減することができる。

[0275] (8) 上記実施の形態において、無効化装置特定部105の無効化装置記憶領域に無効な装置識別子が記憶されていない場合、鍵無効化データ生成部106は、和集合により全装置の装置識別子を含むことのできる2つの部分集合と、それら部分集合に対応するデバイス鍵を、デバイス鍵テーブルD100から読み出し、2つの暗号化メディア鍵を生成したが、これに限定されない。以下のようにして、1つの暗号化メディア鍵を生成してもよい。

[0276] 鍵管理装置100は、全ての装置に共通のラベル「A0」を生成し、生成したラベル「A0」からデバイス鍵「K0」を生成し、ラベル「A0」とデバイス鍵「K0」と全ての装置識別子からなる集合S0とからなる組を情報格納部102に記憶し、鍵管理装置100は、全ての装置に対して、集合S0とラベル「A0」とを予め配布する。

鍵管理装置100は、無効化装置記憶領域に無効な装置識別子が記憶されていない場合、集合S0とデバイス鍵「K0」とを情報格納部102から読み出し、読み出したデバイス鍵「K0」を用いて、暗号化メディア鍵Enc(K0、メディア鍵)を生成する。鍵管理装置100は、生成した暗号化メディア鍵Enc(K0、メディア鍵)と集合S0とを記録媒体200aの鍵無効化データ格納部201へ書き込む。

[0277] これにより、全ての記録装置及び全ての再生装置は、集合S0に対応するラベル「A0」を用いて、デバイス鍵「K0」を生成することができ、暗号化メディア鍵Enc(K0、メディア鍵)を復号して、メディア鍵を生成することができる。

(9) 上記実施の形態において、鍵無効化データ生成部106は、無効化装置特定部105の無効化装置記憶領域に無効な装置識別子が記憶されていない場合と、記憶されている場合との動作を区別したが、これに限定されない。鍵無効化データ生成部106は、無効な装置識別子が記憶されている否かを判断することなく、上記実施にて示す無効な装置識別子が記憶されている場合の動作を行うようにしてもよい。

[0278] このとき、図28にて示す鍵無効化データの生成処理は、ステップS500の実行後、ステップS540を行う。無効化装置記憶領域に無効な装置識別子が記憶されてい

い場合には、ステップS540からステップS555を繰り返すことにより、鍵無効化データ生成部106は、1以上の部分集合を読み出すことができ、全装置それぞれに対応する装置識別子は、読み出した各部分集合の何れかに含まれていることになる。

- [0279] (10) 上記実施の形態において、擬似乱数生成器Gは、Xビットから3Xビットからなる乱数を生成したが、これに限定されない。擬似乱数生成器Gは、Xビットから2Xビットからなる乱数を生成してもよい。

この場合における鍵管理装置100の動作について説明する。

鍵管理装置100は、Xビットからなる乱数Ahを生成すると、生成した乱数Ahをデバイス鍵として、 $(T^2 + T) / 2$ 行、h列に記録する。これにより、 $(T^2 + T) / 2$ 行、h列に記録された部分集合に、乱数Ahをデバイス鍵として割り当てることができる。

- [0280] 鍵管理装置100は、乱数Ah及び擬似乱数生成器Gを用いて、2Xビットからなる乱数を生成する。ここで、生成された2Xビットのうち左Xビットは、乱数Ahに対応する部分集合の子ノードを関連付ける際に、左の子ノードに対応するデバイス鍵であり、右Xビットは、右の子ノードに対応するデバイス鍵である。

鍵管理装置100は、部分集合Sに対する子ノードである1つの部分集合又は2つの部分集合を検出すると、実施の形態にて示したラベルの割り当て方法と同様の方法にて、検出した各部分集合に、擬似乱数生成器Gによって生成されたデバイス鍵を割り当てる。これにより、鍵管理装置100は、部分集合と、デバイス鍵とからなるデバイス鍵テーブル、及び相互関係テーブルを生成することができる。なお、相互関係テーブルの生成は、実施の形態と同様であるため、説明は省略する。

- [0281] このとき、鍵管理装置100が各装置へ配布する鍵情報は、部分集合と、その部分集合に対応するデバイス鍵とからなる。

記録装置300は、鍵情報を用いて、暗号化メディア鍵の復号鍵を取得する場合には、検出部分集合から基準部分集合に至る経路のノード数をZ (Zは2以上) とすると、擬似乱数生成器GをZ-1回利用することで、復号鍵を取得することができる。記録装置300は、擬似乱数生成器GをZ-1回利用して取得した2つのデバイス鍵のうち、基準部分集合が、その親ノードに対して、左の子ノードであるか右の子ノードであるかを判断する。左の子ノードであると判断する場合には、2Xビットのうち左Xビットから

なるデバイス鍵を復号鍵として取得し、右の子ノードであると判断する場合には、右Xビットからなるデバイス鍵を復号鍵として取得する。なお、擬似乱数生成器Gによって生成された2つのデバイス鍵のうち何れのデバイス鍵を次の入力に用いるかの判断は、上記実施の形態と同様であるため、説明は省略する。また、Z=1の場合、つまり検出部分集合と基準部分集合とが同一である場合には、検出部分集合に対応するデバイス鍵を暗号化メディア鍵の復号鍵とする。

[0282] 再生装置400も、上記と同様の動作にて、暗号化メディア鍵の復号鍵を取得する。

(11) 上記実施の形態において、デバイス鍵テーブルD100の各欄には、部分集合、その部分集合に対応するラベル及びそのラベルに対応するデバイス鍵を記録したが、これに限定されない。デバイス鍵テーブルD100の各欄には、部分集合、その部分集合に対応するラベルを記録してもよい。

[0283] このとき、鍵管理装置100は、鍵無効化データを生成する際に、取得した部分集合に対応するラベルを用いて、デバイス鍵を生成し、生成したデバイス鍵を用いて、暗号化メディア鍵を生成する。生成した暗号化メディア鍵と取得した部分集合とを、鍵無効化データとして、記録媒体200aへ記録する。

(12) 上記実施の形態において、鍵情報は、ラベルと、そのラベルに対応する部分集合とからなるとしたが、これに限定されない。部分集合の代わりに、以下に示す経路情報としてもよい。

[0284] 経路情報は、ルート番号と、生成経路とからなる。

ルート番号は、配布するラベルに対応する部分集合が属する木構造のルートとなる部分集合が、相互関係テーブルD101において上位何番目に位置するかを示す。言い換えると、ルートとなる部分集合が、デバイス鍵テーブルD100の最下位行において、左から何番目に位置するかを示す数である。例えば、部分集合「1」をルートする場合には、ルート番号は、「1」となり、部分集合「3」をルートする場合には、ルート番号は、「3」となる。

[0285] 生成経路は、ルートに対する部分集合に割り当てられたラベルから、配布するラベルが生成される経路であり、0、1、2、及び1と2の組合せにより示される。「0」は、ラベルそのもの、つまりルートのノードに割り当てられたラベルを示す。「1」は、親ノードか

ら右へ移動したこと、つまり、子ノードに親ノードにて生成された右及び左ラベルのうち右ラベルを割り当てたことを示し、「2」は、親ノードから左へ移動したこと、つまり、子ノードに親ノードにて生成された右及び左ラベルのうち左ラベルを割り当てたことを示す。例えば、図5に示すラベル「A1」の生成経路は、「0」となり、ラベル「A1RL」の生成経路は、「12」となり、ラベル「A5RLRR」の生成経路は、「1211」となる。

[0286] なお、以降において、経路情報を、「ルート番号ー生成経路」と表記する。

鍵管理装置100の配布部104は、配布指示及び装置識別子を受け取ると、受け取った装置識別子に対する装置へ、配布するラベルと、そのラベルに対応する経路情報とを含む鍵情報を1以上生成して取得する。配布部104は、取得した1以上の鍵情報を受け付けた装置識別子に対応する装置へ配布する。

[0287] ここで、経路情報の取得の動作について、図26及び図27を用いて、変更点のみ説明する。

まず、ステップS445の動作を、検出した部分集合に対応する経路情報が、鍵情報記憶領域に記憶済みであるか否かを判断する動作に変更する。このとき、配布部104は、ステップS450にて、検出した部分集合に対応する経路情報が記憶済みでないと判断する場合には、ステップS450を実行する。

[0288] 次に、ステップS455を以下のように変更する。

(変更内容)配布部104は、検出したノード、つまり木構造Viのルートであるか否かを判断する。ルートであると判断する場合には、生成経路を「0」とする。ルートでないと判断する場合には、ルートから検出したノードに至る生成経路を取得する。さらに、配布部104は、木構造Viのルートに対するルート番号を取得する。この場合、iが、ルート番号となる。配布部104は、取得したルート番号と生成経路とからなる経路情報を生成し、生成した経路情報と、読み出したラベルとを含む鍵情報を生成して取得する。

[0289] 次に、ステップS475を省略し、ステップS480の動作を、全ての鍵情報を、受け取った端末装置識別子に対応する装置へ配布するように変更する。なお、ここで、配布とは、例えば、配布用の記録媒体に、受け付けた装置識別子と、鍵情報記憶領域にて記憶している1以上の鍵情報との書き込みが完了したことをいう。

また、鍵管理装置100は、鍵無効化データを生成する場合には、先ず、上記実施の形態と同様に、無効化装置記憶領域の記憶内容に基づいて、1以上の部分集合を取得する。取得した各部分集合に対応するラベル及びデバイス鍵を取得する。鍵管理装置100は、取得した各デバイス鍵を用いて、暗号化メディア鍵をそれぞれ生成する。さらに、鍵管理装置100は、取得した各部分集合が属するそれぞれの本構造を用いて、経路情報を取得する。取得方法は、先ず、部分集合が属するルートの部分集合を取得し、取得したルートの部分集合と、相互関係テーブルD101とを用いて、ルート番号を取得する。さらに、ルートから取得したラベルの部分集合までに至る経路より生成経路を取得し、取得したルート番号と生成経路より経路情報を生成する。生成経路の取得は、上記と同様である。鍵管理装置100は、生成した各経路情報と、各暗号化メディア鍵とを対応付けて、鍵無効化データを生成し、生成した各鍵無効化データを、記録媒体200aへ書き込む。例えば、装置4及び装置5が無効化される場合には、鍵管理装置100は、部分集合「123」及び部分集合「678」を取得し、さらには、各部分集合に対応するデバイス鍵「K3」、「K33」と、各部分集合に対応するラベルに対する経路情報「1-12」、「7-11」を取得する。

[0290] また、装置4及び装置5が無効化された場合に、記録媒体200bにて記憶されている鍵無効化データを、図39に示す。鍵無効化データは、上述したように、暗号化メディア鍵と、メディア鍵の暗号化の用いたデバイス鍵に対応するラベルの経路情報とからなる。装置4及び装置5が無効化された場合には、記録媒体200bは、上述したように、2つの鍵無効化データを記憶することになる。

[0291] また、各装置が、保持する鍵情報を図40にて示す。鍵情報の上段は、経路情報を示し、下段には、ラベルを示す。

ここで、記録装置300にて行われる暗号化メディア鍵の復号について、図29、図30及び図31を用いて、変更点のみ説明する。なお、第1及び第2暗号化処理については、上記実施の形態と同様であるため、説明は省略する。

[0292] <記録処理の変更点>

先ず、ステップS605の動作を、入出力部309を介して当該記録装置300に装着された記録媒体200bより、記録媒体200bに記録されている1以上の暗号化メディア

鍵のそれぞれに対応する経路情報のうち、1つの経路情報(以下、基準経路情報という。)を読み出す動作に変更する。

[0293] 次に、ステップS610の動作を、1以上の鍵情報の読み出す動作に変更する。

次に、ステップS615を以下のように変更する。

(変更内容)復号鍵生成部304は、読み出した1以上の鍵情報から、基準経路情報のルート番号(以下、基準ルート番号という。)と一致するルート番号をもち、且つ「0」からなる生成経路をもつ又は基準経路情報に含まれる生成経路(以下、基準生成経路という。)に対して左前方一致する生成経路をもつ経路情報(以下、検出経路情報という。)を検索する。ここで、左前方一致について、説明する。まず、生成経路にて表記される数字の個数を、生成経路の長さとする。例えば、生成経路「2」は、長さ1であり、背製経路「12121」は、長さ5である。左前方一致とは、基準生成経路をp1、生成経路をp2とした場合、 $p1=p2$ 又は $p1=p2 \mid \mid p3$ となることである。ここで、p3の長さは1以上である。例えば、生成経路「1」及び「121」は、それぞれ生成経路「12」及び「1211」に対して左前方一致している。なお、検索方法については、具体例を用いて、後述する。

[0294] 次に、ステップS620の動作を、検出経路情報を検出したか否かを判断する動作に変更する。ステップS625の動作を、未読出の基準経路情報は存在するか否かを判断する動作に変更する。さらに、ステップS630の動作を、基準経路情報を読み出す動作に変更する。

ここで、検索方法について、具体例を用いて、説明する。なお、記録装置300に装着される記録媒体200bは、図39に示す2つの鍵無効化データを記憶しているとする。記録装置300は装置識別子2を有している場合には、復号鍵生成部304は、基準ルート番号「1」が、読み出した各鍵情報に含まれる経路情報に存在するか否かを判断する。ここでは、存在すると判断し、経路情報「1-1」を取得する。次に、生成経路が「0」である可否かを判断する。ここでは、「0」でないと判断する。次に、復号鍵生成部304は、取得した経路情報「1-1」の生成経路「1」が、基準生成経路に対して左前方一致しているか否かを判断する。ここでは、一致していると判断し、経路情報「1-0」を検出経路情報として検出することになる。

[0295] 記録装置300は装置識別子7を有している場合には、復号鍵生成部304は、基準ルート番号「1」をもつ経路情報を記録装置300は保持していないため、記録媒体200bより、次の、基準経路情報「7-11」を読み出す。復号鍵生成部304は、基準ルート番号「7」が、読み出した各鍵情報に含まれる経路情報に存在するか否かを判断する。ここでは、存在すると判断し、経路情報「7-0」を取得する。次に、生成経路が「0」である可否かを判断する。ここでは、「0」であると判断し、経路情報「7-0」を検出経路情報として検出することになる。

[0296] <デバイス鍵の取得処理の変更点>

先ずステップS700の動作を、検出経路情報に対応するラベルを取得する動作に変更する。

次に、ステップS705の動作を、基準生成経路の長さ、検出生成経路の長さの差分Zを取得する動作に変更する。

[0297] ステップS710からステップS740までの繰り返しの制御を、 $z=1-Z+1$ までの間、行うように変更する。

ステップS720の判断動作を、基準生成経路において、「検出生成経路の長さ+z」番目に数字が存在するか否かを判断する動作に変更する。

ステップS725の判断動作を、「検出生成経路の長さ+z」番目に存在する数字が2であるか否かを判断する動作に変更する。

[0298] ステップS745の動作を、Z+1回目に取得した乱数よりデバイス鍵を取得する動作に変更する。

ステップS750の動作を、デバイス鍵及び基準経路情報を復号部305へ出力する動作に変更する。

<復号処理の変更点>

ステップS800の動作を、デバイス鍵及び基準経路情報を受け取る動作に変更する。

[0299] ステップS805の動作を、基準経路情報に対応する暗号化メディア鍵を取得する操作に変更する。

以上の点を変更することにより、記録装置300は、ラベル及び経路情報からなる鍵

情報を用いて、暗号化メディア鍵を復号して、メディア鍵を生成することができる。

なお、再生装置400にて行われる暗号化メディア鍵の復号についても、図34、図35及び図36に示す各処理に対して、上記に示す変更と同様の変更を行えばよいため、説明は省略する。

[0300] (13) 上記(12)において、鍵管理装置100は、鍵情報の配布時、及び鍵無効化データの生成時に、経路情報を生成したが、これに限定されない。デバイス鍵の生成時に、経路情報を生成し、デバイス鍵テーブルD100へ、生成した経路情報、部分集合、ラベル及びデバイス鍵からなる組を記録してもよい。これにより、鍵情報の配布時、及び鍵無効化データの生成時においては、経路情報をデバイス鍵テーブルD100より読み出すだけでよい。

[0301] (14) 上記実施の形態において、レイヤ0で生成された1個の部分集合とレイヤ1で生成された1個の部分集合との関連付け、及びレイヤ1で生成された1個の部分集合とレイヤ2で生成された1個の部分集合との関連付けを行ったが、これに限定されない。

例えば、レイヤ0で生成された1個の部分集合とレイヤ1で生成された1個の部分集合との関連付けのみを行ってもよい。

[0302] この場合、装置1へ配布するラベルは、部分集合「1」、部分集合「12」、部分集合「123」、部分集合「125678」及び部分集合「1345678」と、それぞれに対応するラベルとからなる5個の鍵情報となり、配布する鍵情報の個数は、従来よりも少なくなる。

または、レイヤ1で生成された1個の部分集合とレイヤ2で生成された1個の部分集合との関連付けのみを行ってもよい。

[0303] この場合も同様に、装置1へ配布する鍵情報の個数は、従来の個数よりも少なくなることが分かる。

(15) 本発明は、生成した複数の部分集合の関連付けは、上記の実施の形態にて示す方法であるとしてもよい。

または、各レイヤ間にて生成した1以上の部分集合を関連付け、各レイヤにおいて部分集合の関連付けがなされた後、レイヤ間における部分集合の関連付けを行ってもよい。

- [0304] 例えば、鍵管理装置100は、図10に示すデバイス鍵テーブルD100aを生成した後、先ず、レイヤ0のノードをルートする木構造から生成された各部分集合、つまりデバイス鍵テーブルD100aにおける1行目501、2行目502及び3行目503に記録される各部分集合を用いて、ルートとして、最小の要素数からなる部分集合とし、子ノードとして、その親ノードを含み、且つ最小の要素数からなる部分集合とする木構造を2つ生成する。つまり、部分集合「1234」をルートする木構造と、部分集合「5678」をルートする木構造とを生成する。
- [0305] 次に、鍵管理装置100は、レイヤ1のノードをルートする木構造から生成された各部分集合、つまりデバイス鍵テーブルD100aにおける4行目504及び5行目505に記録される各部分集合を用いて、ルートとして、最小の要素数からなる部分集合とし、子ノードとして、その親ノードを含み、且つ最小の要素数からなる部分集合とする木構造を4つ生成する。
- [0306] さらに、鍵管理装置100は、レイヤ2のノードをルートする木構造から生成された各部分集合、つまりデバイス鍵テーブルD100aにおける6行目506に記録される各部分集合を用いて、ルートとして、最小の要素数からなる部分集合とし、子ノードとして、その親ノードを含み、且つ最小の要素数からなる部分集合とする木構造を8つ生成する。ここで生成される8つの木構造は、ルートのみからなる木構造である。
- [0307] 次に、生成した各木構造を用いて、木構造間の関連付けを以下のように行う。先ず、部分集合「1」をルートする木構造と、部分集合「1」を含み、且つ最小の要素数からなる部分集合をルートする木構造、ここでは、部分集合「12」をルートする木構造とを関連付ける。さらに、部分集合「12」をルートする木構造と、当該木構造の1つのリーフ、ここでは、部分集合「123」を含み、且つ最小の要素数からなる部分集合をルートする木構造、ここでは、部分集合「1234」をルートする木構造とを関連付ける。この動作を1個の要素からなる各部分集合の個数分繰り返すことにより、図11にて示す各部分集合の相互関連と同様の相互関連がなされる。なお、1度関連付けがなされた部分集合木構造は、他の関連付けには利用しない。
- [0308] (16) 上記実施の形態において、部分集合の木構造の構成中、つまり相互関係テーブルの生成中に、木構造の各ノードに対するラベルを割り当てたが、これに限定さ

れない。各ノードに割り当てるラベルは、部分集合の木構造の構成が完了した後、つまり相互関係テーブルの作成が完了した後に、割り当ててもよい。

(17)本発明は、上記に示す方法であるとしてもよい。また、これらの方法をコンピュータにより実現するコンピュータプログラムであるとしてもよいし、前記コンピュータプログラムからなるデジタル信号であるとしてもよい。

[0309] また、本発明は、前記コンピュータプログラム又は前記デジタル信号をコンピュータ読み取り可能な記録媒体、例えば、フレキシブルディスク、ハードディスク、CD-ROM、MO、DVD、DVD-ROM、DVD-RAM、BD(Blu-ray Disc)、半導体メモリなど、に記録したものとしてもよい。また、これらの記録媒体に記録されている前記コンピュータプログラム又は前記デジタル信号であるとしてもよい。

[0310] また、本発明は、前記コンピュータプログラム又は前記デジタル信号を、電気通信回線、無線又は有線通信回線、インターネットを代表とするネットワーク等を経由して伝送するものとしてもよい。

また、本発明は、マイクロプロセッサとメモリとを備えたコンピュータシステムであって、前記メモリは、上記コンピュータプログラムを記憶しており、前記マイクロプロセッサは、前記コンピュータプログラムに従って動作するとしてもよい。

[0311] また、前記プログラム又は前記デジタル信号を前記記録媒体に記録して移送することにより、又は前記プログラム又は前記デジタル信号を前記ネットワーク等を経由して移送することにより、独立した他のコンピュータシステムにより実施するとしてもよい。

(18)上記実施の形態及び上記変形例をそれぞれ組み合わせるとしてもよい。

1. 10 まとめ

鍵管理装置は、複数の端末装置から、いくつかを任意に選んで、複数の許可集合を生成し、許可集合毎に、1の鍵が割り当てられる。許可集合に割り当てられた鍵により、データが暗号化され、許可集合の含まれる端末装置は、その暗号化されたデータを利用できる。第1許可集合と他の第2許可集合とが関連付けられている。関連付けにより第1許可集合の鍵から、第2許可集合の鍵が生成される。鍵管理装置は、前記複数の端末装置を、複数のグループに分ける。1のグループについて、グループ

に含まれる複数の端末装置から、いくつかを任意に選んで、複数の許可集合を生成する。許可集合毎に、1の鍵が割り当てられ、許可集合に割り当てられた鍵により、データが暗号化され、許可集合に含まれる端末装置は、その暗号化されたデータを利用できる。第3許可集合と他の第4許可集合とが関連付けられている。関連付けにより第3許可集合の鍵から、第4許可集合の鍵が生成される。鍵管理装置は、第1許可集合と第4許可集合を関連付ける。

[0312] ここで、非特許文献1における各部分集合の関係について、説明する。非特許文献1における各部分集合の関係は、レイヤ i (i は0以上)の存在するノードをルートする部分木から生成された複数の部分集合について、本発明と同様の関連付けがなされる。例えば、図3に示すE1をルートする部分木からは、部分集合「12」、「123」、「124」、「34」、「134」及び「234」が生成され、各部分集合の関連付けは、図11に示すように、部分集合「12」と、部分集合「123」及び「124」とを関連付け、部分集合「34」と、部分集合「134」及び「234」とを関連付ける。しかしながら、2つの部分木にまたがって、部分集合の関連付けがなされていない。従って、各部分木は、それぞれ独立の関係にある。

[0313] つまり、非特許文献1における各部分集合の関係は、図11に示す関係から、部分集合「1」と部分集合「12」との関連付け、部分集合「123」と部分集合「1234」との関連付け、部分集合「3」と部分集合「34」との関連付け、部分集合「5」と部分集合「56」との関連付け、部分集合「567」と部分集合「5678」との関連付け、及び部分集合「7」と部分集合「78」との関連付けがなされていない状態である。従って、従来技術では、例えば、装置1へは、部分集合「1」のラベル、部分集合「12」のラベル、部分集合「134」のラベル、部分集合「1234」のラベル、部分集合「125678」のラベル及び部分集合「1345678」のラベルの計6個のラベルを配布する必要がある。

[0314] しかしながら、本発明によると、2つのルートが親子関係となる2つのノードにおいてそれぞれをルートする2つの部分木のうち、子ノードをルートする部分木から生成される複数の部分集合のうち最大の要素数を持つ部分集合F1と、親ノードをルートとする部分から生成される複数の部分集合のうち、部分集合F1を含み、且つ最小の要素数からなる部分集合F2との間との関連付けを行っている。従って、2つの部分木にま

たがって、部分集合の関連付けがなされ、部分木間の関連付けがなされる。これにより、配布するラベルの数を削減することができる。

[0315] 例えば、部分集合「1」と部分集合「12」とを関連付けることにより、図41に示すように、木構造T100におけるノードT510「E3」をルートとする部分木T501と、ノードT511「E1」をルートとする部分木T502との関連付けがされ、部分木T502にて生成される部分集合「12」、部分集合「123」及び部分集合「124」のそれぞれに対応する各ラベルは、部分木T501にて生成される部分集合「1」に対応するラベルから、擬似乱数生成器G150を用いて生成されることになる。また、部分集合「123」と部分集合「1234」とを関連付けることにより、図41に示すように、ノードT511「E1」をルートとする部分木T502と、ノードT512「E0」をルートとする部分木T503との関連付けがされ、部分木T503にて生成される部分集合「1234」、部分集合「123456」、部分集合「124123478」、部分集合「1234567」、部分集合「1234568」、部分集合「1234578」及び部分集合「1234678」のそれぞれに対応する各ラベルは、部分木T502にて生成される部分集合「123」に対応するラベル、つまり部分木T501にて生成される部分集合「1」に対応するラベルから、擬似乱数生成器G150を用いて生成されることになる。従って、鍵管理装置100は、装置1に対しては、部分集合「12」のラベル及び部分集合「1234」のラベルを配布する必要が無く、部分集合「1」のラベル、部分集合「134」のラベル、部分集合「125678」のラベル及び部分集合「1345678」のラベルの計4個のラベルを配布すればよい。

[0316] さらに、非特許文献1における技術では、各装置を管理する木構造の各ノード、つまり、部分木の各ルートに対して、異なるラベルを割り当てる必要があるが、本発明では、上述したように、部分木間の関連付けを行うため、部分木の各ルートに対して異なるラベルを割り当てる必要がない。つまり、異なるラベルの数を従来よりも少なくすることができる。

[0317] さらに、鍵管理装置100は、鍵無効化データを生成することにより、不正な装置が持つラベルでは、コンテンツの記録、あるいは再生に必要な鍵が算出できず、不正装置以外の1以上の正規装置では、各装置が有するラベルを用いて、コンテンツの記録、あるいは再生に必要な鍵が算出できる。

非特許文献1に開示されている従来の鍵無効化技術では、装置の数が増大すると、各装置が内蔵するラベルの数が膨大になるという課題がある。例えば、装置数が約10億台(高さ30の2分木)のシステムを考えた場合、各装置が保持するラベルの数は465個となる。しかしながら、本発明によれば、各装置が内蔵する鍵の数を削減することが可能である。具体的には、木構造の高さを T 、当該システムに属する装置の総数を Q 台とした場合、 $Q/2$ 台の装置において $T-1$ 個の鍵が削減され、 $Q/4$ 台の装置において $T-2$ 個の鍵が削減され、 $Q/(2^k)$ 台の装置において $T-k$ 個の鍵が削減される。ただし、 k は1以上、且つ $T-1$ 以下の整数である。

[0318] 本発明にかかる鍵無効化システムは、各装置が保持するラベル、つまり鍵に対して相互関係を持たせることにより、各装置が持つラベル、つまり鍵の数を削減することができるという効果を有し、同一システムにおいて、据え置き機や携帯端末などが混在する場合に、記憶容量の小さい携帯端末に対しては保持する鍵が少なくなるように割り当てることができるため、鍵無効化を実現するシステムにおいて有用である。

[0319] 本発明は、特定の装置を無効化するための無効化情報の生成を行い配布する鍵管理装置と、前記無効化情報を記録する記録媒体と、前記記録媒体から前記無効化情報を読み出して処理する端末装置からなる著作権保護システムであって、前記鍵管理装置は、前記著作権保護システムに属する端末装置の部分集合を生成する部分集合生成部と、前記部分集合に対して鍵を割り当てる割当部と、前記部分集合が含まれる他の部分集合の鍵を前記割り当てた鍵から生成する鍵生成部と、前記部分集合に割り当てた鍵に基づいて無効化情報を生成する無効化情報生成部を備えることを特徴とする。

[0320] また、本発明は、前記著作権保護システムであって、前記鍵管理装置の鍵生成部は、前記部分集合に割り当てられた鍵から、一方向性関数を利用して他の部分集合の鍵を生成することを特徴とする。

また、本発明は、前記著作権保護システムであって、前記鍵管理装置の鍵生成部は、前記部分集合に割り当てられた鍵から、複数の他の部分集合の鍵を生成することを特徴とする。

[0321] また、本発明は、前記著作権保護システムであって、前記鍵管理装置は、前記部

分集合と割り当てた鍵の対応関係、並びに生成された鍵の相互関係を記憶する記憶部を備えることを特徴とする。

また、本発明は、前記著作権保護システムであって、前記鍵管理装置の記憶部は、前記部分集合と割り当てた鍵の対応関係、並びに生成された鍵の相互関係を、テーブルを利用して管理し、前記テーブルを記憶することを特徴とする。

[0322] また、本発明は、前記著作権保護システムであって、前記鍵管理装置は、前記部分集合に対して割り当てた鍵を前記端末装置に配布する鍵配布部を備え、前記鍵配布部は、鍵を配布する端末装置が含まれる部分集合のうち、最小の部分集合を選択して、前記選択した部分集合に割り当てられた鍵を配布し、さらに、前記配布した鍵から生成される鍵が割り当てられた部分集合を除く部分集合から、前記端末装置が含まれる最小の部分集合を選択して、前記選択した部分集合に割り当てられた鍵を配布することを特徴とする。

[0323] また、本発明は、前記著作権保護システムであって、前記鍵管理装置の無効化情報生成部は、有効な端末装置だけが含まれる最大の部分集合を選択して、前記選択した部分集合に含まれない端末装置に対しては、さらに、それら端末装置だけが含まれる最大の部分集合を選択して、前記選択を、全ての有効な端末装置が何れかの部分集合に含まれるまで繰り返し行うことを特徴とする。

[0324] また、本発明は、前記著作権保護システムであって、前記端末装置は、前記無効化情報を処理する鍵を格納する格納部を備え、前記格納部には、自身が含まれる部分集合に割り当てられた鍵を格納することを特徴とする。

また、本発明は、前記著作権保護システムであって、前記端末装置の格納部は、鍵と部分集合の対応関係を示す情報も合わせて格納することを特徴とする。

[0325] また、本発明は、前記著作権保護システムであって、前記端末装置の格納部は、ある部分集合に割り当てられた鍵から、他の部分集合の鍵が生成可能な場合、前記生成可能な鍵は格納しないことを特徴とする。

また、本発明は、前記著作権保護システムであって、前記端末装置は、前記格納部に格納する鍵から、他の部分集合に割り当てられた鍵を生成する鍵生成部を備え、前記鍵生成部は、部分集合と鍵の対応関係、並びに生成された鍵の相互関係から

他の部分集合に割り当てられた鍵を生成することを特徴とする。

[0326] また、本発明は、前記著作権保護システムであって、前記端末装置は、前記記録媒体に対して、暗号化されたコンテンツを記録する記録部を備えることを特徴とする。

また、本発明は、前記著作権保護システムであって、前記端末装置は、前記記録媒体から暗号化されたコンテンツを読み出して復号、及び再生する再生部を備えることを特徴とする。

[0327] また、本発明は、前記著作権保護システムであって、前記鍵管理装置が生成した無効化情報には、どの部分集合の鍵に基づいて生成したのかを示す情報が付与されることを特徴とする。

また、本発明は、前記著作権保護システムであって、前記記録媒体の代わりに通信媒体を利用することを特徴とする。

[0328] また、本発明は、特定の装置を無効化するための無効化情報の生成を行い配布する鍵管理装置であって、前記鍵管理装置は、前記著作権保護システムに属する端末装置の部分集合を生成する部分集合生成部と、前記部分集合に対して鍵を割り当てる割当部と、前記部分集合が含まれる他の部分集合の鍵を前記割り当てた鍵から生成する鍵生成部と、前記部分集合に割り当てた鍵に基づいて無効化情報を生成する無効化情報生成部を備えることを特徴とする。

[0329] また、本発明は、前記鍵管理装置であって、前記鍵生成部は、前記部分集合に割り当てられた鍵から、一方向性関数を利用して他の部分集合の鍵を生成することを特徴とする。

また、本発明は、前記鍵管理装置であって、前記鍵生成部は、前記部分集合に割り当てられた鍵から、複数の他の部分集合の鍵を生成することを特徴とする。

また、本発明は、前記鍵管理装置であって、前記部分集合と割り当てた鍵の対応関係、並びに生成された鍵の相互関係を記憶する記憶部を備えることを特徴とする。

[0330] また、本発明は、前記鍵管理装置であって、前記記憶部は、前記部分集合と割り当てた鍵の対応関係、並びに生成された鍵の相互関係を、テーブルを利用して管理し、前記テーブルを記憶することを特徴とする。

また、本発明は、前記鍵管理装置であって、前記部分集合に対して割り当てた鍵を

前記端末装置に配布する鍵配布部を備え、前記鍵配布部は、鍵を配布する端末装置が含まれる部分集合のうち、最小の部分集合を選択して、前記選択した部分集合に割り当てられた鍵を配布し、さらに、前記配布した鍵から生成される鍵が割り当てられた部分集合を除く部分集合から、前記端末装置が含まれる最小の部分集合を選択して、前記選択した部分集合に割り当てられた鍵を配布することを特徴とする。

[0331] また、本発明は、前記鍵管理装置であって、前記無効化情報生成部は、有効な端末装置だけが含まれる最大の部分集合を選択して、前記選択した部分集合に含まれない端末装置に対しては、さらに、それら端末装置だけが含まれる最大の部分集合を選択して、前記選択を、全ての有効な端末装置が何れかの部分集合に含まれるまで繰り返し行うことを特徴とする。

[0332] また、本発明は、記録媒体から無効化情報を読み出して処理する端末装置であって、前記端末装置は、前記無効化情報を処理する鍵を格納する格納部を備え、前記格納部には、自身が含まれる部分集合に割り当てられた鍵を格納することを特徴とする。

また、本発明は、前記端末装置であって、前記格納部は、鍵と部分集合の対応関係を示す情報も合わせて格納することを特徴とする。

[0333] また、本発明は、前記端末装置であって、前記格納部は、ある部分集合に割り当てられた鍵から、他の部分集合の鍵が生成可能な場合、前記生成可能な鍵は格納しないことを特徴とする。

また、本発明は、前記端末装置であって、前記端末装置は、前記格納部に格納する鍵から、他の部分集合に割り当てられた鍵を生成する鍵生成部を備え、前記鍵生成部は、部分集合と鍵の対応関係、並びに生成された鍵の相互関係から他の部分集合に割り当てられた鍵を生成することを特徴とする。

[0334] また、本発明は、前記端末装置であって、前記端末装置は、前記記録媒体に対して、暗号化されたコンテンツを記録する記録部を備えることを特徴とする。

また、本発明は、前記端末装置であって、前記端末装置は、前記記録媒体から暗号化されたコンテンツを読み出して復号、及び再生する再生部を備えることを特徴とする。

また、本発明は、特定の装置を無効化するための無効化情報を記録する記録媒体であって、鍵管理装置は、著作権保護システムに属する端末装置の部分集合を生成する部分集合生成部と、前記部分集合に対して鍵を割り当てる割当部と、前記部分集合が含まれる他の部分集合の鍵を前記割り当てた鍵から生成する鍵生成部と、前記部分集合に割り当てた鍵に基づいて無効化情報を生成する無効化情報生成部を備え、前記鍵管理装置により生成された無効化情報を記録することを特徴とする。

[0335] また、本発明は、前記記録媒体であって、前記鍵管理装置が生成した無効化情報には、どの部分集合の鍵に基づいて生成したのかを示す情報が付与されており、前記付与された情報と共に前記鍵無効化情報を記録することを特徴とする。

産業上の利用可能性

[0336] 発明を構成する各装置及び記録媒体は、電器機器製造産業において、経営的に、また継続的及び反復的に、製造し、販売することができる。また、本発明を構成する各装置及び記録媒体は、コンテンツを制作し、配給するコンテンツ配給産業において、経営的に、また継続的及び反復的に使用することができる。

請求の範囲

- [1] 複数の端末装置を識別する各装置識別子を木構造のリーフに配し、各装置識別子に、暗号化されたデータを復号する復号鍵の基となる固有情報を割り当て、管理する管理装置であって、
- 前記木構造のリーフを除く各レイヤのノードにおいて、その配下に存する装置識別子の部分集合を求めて、生成する部分集合生成手段と、
- リーフのレイヤを除く最下位レイヤの部分集合をそっくり含む部分集合を直上位のレイヤから検索し、関連付ける第1関連付手段と、
- 関連付先の部分集合をそっくり含む部分集合を同一レイヤ及び直上位のレイヤの何れかから検索し、関連付ける第2関連付手段と、
- 最上位レイヤに至るまで、前記第2関連付手段が繰り返し処理するよう制御する第1制御手段と、
- 前記最下位レイヤの部分集合の全てに対して、前記第1関連付手段、前記第2関連付手段、及び前記第1制御手段が繰り返し処理するよう制御する第2制御手段と、
- 前記最下位レイヤの関連付元の部分集合に、固有情報を対応付けて、当該固有情報を、当該部分集合に含まれる装置識別子に割り当てる第1割当手段と、
- 関連付けにより、レイヤにまたがって繋がった部分集合に、前記関連付元の部分集合に割り当てた固有情報から派生的に求められる固有情報を対応付けて、当該固有情報を、当該部分集合に含まれる各装置識別子に割り当てる第2割当手段と
- を備えることを特徴とする管理装置。
- [2] 前記第1関連付手段は、前記最下位レイヤの部分集合をそっくり含み、且つ最小の要素数からなる部分集合を検索し、前記最下位レイヤの部分集合を親ノードとし、検索した部分集合を子ノードとして、関連付け、
- 前記第2関連付手段は、前記関連付先の部分集合をそっくり含み、且つ最小の要素数からなる部分集合を検索し、前記関連付先の部分集合を親ノードとし、検索した部分集合を子ノードとして、関連付け、
- 前記第1制御手段は、最上位レイヤに至るまで、前記第2関連付手段が繰り返し処理するよう制御して、前記最下位レイヤの部分集合をルートする部分集合木を生成

する

ことを特徴とする請求項1に記載の管理装置。

- [3] 前記第1関連付手段は、前記最下位レイヤに対する各上位レイヤの各部分集合のうち、関連付けがなされた1以上の部分集合を除外し、残りの1以上の部分集合を用いて、最上位レイヤに至るまで、前記第2関連付手段が繰り返し処理するよう制御して、前記最下位レイヤの部分集合をルートする部分集合木を生成する

ことを特徴とする請求項2に記載の管理装置。

- [4] 前記第2割当手段は、

前記派生的に求められる固有情報を、前記関連付元の部分集合に対応付けされた固有情報から一方向性関数を用いて生成し、生成した固有情報を、関連付けにより繋がった部分集合に対応付ける

ことを特徴とする請求項3に記載の管理装置。

- [5] 前記管理装置は、さらに、

前記部分集合木のルートから1以上のリーフそれぞれに至る各経路において、固有情報を配布する配布対象の端末装置の識別子が、要素として初めて出現する部分集合が存在する場合に、前部分集合に対応付けられた固有情報を1以上取得する固有情報取得手段と、

取得した固有情報と、固有情報に対応する部分集合を識別する集合識別情報とからなる1以上の組を、前記配布対象の端末装置へ配布する配布手段と

を備えることを特徴とする請求項4に記載の管理装置。

- [6] 前記固有情報取得手段は、

部分集合木のルートからリーフに至る各経路から、前記配布対象の端末装置の識別子が、要素として初めて出現する部分集合を検索し、前記部分集合を検出すると、前記検出した部分集合が未取得である場合に、前記検出した部分集合を取得する第1取得部と、

第1取得部にて取得した前記部分集合に対応付けられた前記固有情報を取得する第2取得部と、

前記各経路に対して行われるまで、前記第1及び第2取得部が繰り返し処理するよ

う制御する繰返制御部と

を備えることを特徴とする請求項5に記載の管理装置。

[7] 前記管理装置は、さらに、

前記部分集合木の構成要素である各部分集合と、前記各部分集合のそれぞれに対応付けられた前記固有情報とを記憶する領域を有する第1記憶手段と、

前記部分集合木を構成する複数のノードと、各ノードの子ノードとを記憶する領域を有する第2記憶手段と、

前記部分集合と、前記部分集合に対応付けられた固有情報とを対応付けて、前記第1記憶手段に書き込む第1書込手段と、

前記部分集合木を構成する前記ノードと、前記ノードの子ノードとを対応付けて、前記第2記憶手段に書き込む第2書込手段と

を備えることを特徴とする請求項5に記載の管理装置。

[8] 前記第1記憶手段は、前記部分集合と前記部分集合に対応付けられた固有情報とを1の組として、複数個の組を記憶する第1テーブルを有しており、

前記第2記憶手段は、前記ノードと前記ノードに対応する子ノードとを1の組として、複数個の組を記憶する第2テーブルを有しており、

前記第1書込手段は、前記部分集合と、前記部分集合に対応付けられた固有情報とからなる組を、前記第1テーブルに書き込み、

前記第2書込手段は、前記ノードと、前記ノードの子ノードとからなる組を、前記第2記憶手段に書き込む

ことを特徴とする請求項7に記載の管理装置。

[9] 前記第2制御手段は、前記最下位レイヤの部分集合の全てに対して、前記第1関連付手段、前記第2関連付手段、及び前記第1制御手段が繰返し処理するよう制御して、複数の部分集合木を生成し、

前記第1記憶手段は、各部分集合木に含まれる各部分集合と、前記各部分集合のそれぞれに対応付けられた各固有情報とを記憶しており、

前記管理装置は、さらに、

前記複数の端末装置のうち、1以上の無効な端末を示す無効な識別子を記憶する

領域を有する無効化識別子記憶手段と、

前記無効化識別子記憶手段にて記憶されている内容に基づいて、前記第1記憶手段より1以上の部分集合を取得し、取得した各部分集合のそれぞれに対応付けられた各固有情報に基づいて、1以上の暗号化鍵を取得し、取得した各暗号化鍵を個別に用いて、コンテンツの利用に用いるメディア鍵を暗号し、前記1以上の暗号化鍵と同数の暗号化メディア鍵を生成する暗号化鍵生成手段と、

前記暗号化メディア鍵と、前記暗号化メディア鍵に対する暗号化鍵の取得に用いられた部分集合を識別する基準識別情報とからなる1以上の組を、当該管理装置に装着された記録媒体へ書き込む第3書込手段と

を備えることを特徴とする請求項7に記載の管理装置。

[10] 前記管理装置は、さらに、

無効な識別子を受け取り、受け取った無効な識別子を前記無効化識別子記憶手段へ書き込む無効化識別子受取手段

を備えることを特徴とする請求項9に記載の管理装置。

[11] 前記暗号化鍵は、前記復号鍵と同一の共通鍵であり、

前記一方向性関数は、さらに、各固有情報から前記各固有情報に基づく各共通鍵を生成し、

前記暗号化鍵生成手段は、

前記無効化識別子記憶手段にて記憶されている無効な識別子を除く1以上の有効な識別子を最も多く含む部分集合を、前記第1記憶手段より取得する部分集合取得部と、

全ての有効な識別子が、前記部分集合取得部にて取得される1以上の部分集合の何れかに属するまで、前記部分集合取得部が繰り返し処理するよう制御する制御部と、

前記一方向性関数を用いて、前記部分集合取得部にて取得した各部分集合のそれぞれに対応付けられた各固有情報から生成された1以上の共通鍵を取得する共通鍵取得部と、

前記共通鍵取得部にて取得した各共通鍵を用いて、共通鍵の数と同数の暗号化メ

ディア鍵を生成する暗号化部と

を備えることを特徴とする請求項9に記載の管理装置。

- [12] 前記基準識別情報は、前記暗号化メディア鍵に対する共通鍵の取得に用いられた部分集合であり、

前記第3書込手段は、前記暗号化メディア鍵と、前記暗号化メディア鍵に対する共通鍵の取得に用いられた部分集合とからなる1以上の組を、前記記録媒体へ書き込み、

前記配布手段は、前記取得した固有情報が対応付けられた部分集合を前記集合識別情報として、前記取得した固有情報と前記集合識別情報とからなる1以上の組を、前記配布対象の端末装置へ配布し、

前記配布手段は、さらに、前記各部分集合木を示すデータ構造を配布することを特徴とする請求項9に記載の管理装置。

- [13] 前記管理装置は、さらに、

部分集合に対して、前記部分集合が属する部分集合木のルートであるルート部分集合から、前記部分集合に至るまでの経路を示す生成経路と、前記ルート部分集合と示すルート識別子とを含む経路情報を取得する経路情報取得手段を備え、

前記基準識別情報は、前記暗号化メディア鍵に対する暗号化鍵の取得に用いられた部分集合の経路情報であり、

前記第3書込手段は、前記暗号化メディア鍵と、前記暗号化メディア鍵に対する暗号化鍵の取得に用いられた部分集合の経路情報とからなる1以上の組を、前記記録媒体へ書き込み、

前記配布手段は、前記取得した固有情報に対する部分集合の経路情報を前記集合識別情報として、前記取得した固有情報と前記集合識別情報とからなる1以上の組を、前記配布対象の端末装置へ配布する

ことを特徴とする請求項9に記載の管理装置。

- [14] 複数の端末装置を識別する各装置識別子を木構造にて管理する管理装置より、暗号化されたデータを復号する復号鍵の基となる固有情報が割り当てられる端末装置であって、

前記管理装置は、

前記木構造のリーフを除く各レイヤのノードにおいて、その配下に存する装置識別子の部分集合を求めて、生成し、リーフのレイヤを除く最下位レイヤの部分集合をそっくり含む部分集合を直上位のレイヤから検索し、関連付け、関連付先の部分集合をそっくり含む部分集合を同一レイヤ及び直上位のレイヤの何れかから検索し、関連付け、この関連付けを最上位レイヤに至るまで、前記第2関連付手段が繰り返し処理するよう制御し、前記最下位レイヤの部分集合の全てに対して、これらの処理が繰り返し処理するよう制御し、前記最下位レイヤの関連付元の部分集合に、固有情報を対応付けて、当該固有情報を、当該部分集合に含まれる装置識別子に割り当て、関連付けにより、レイヤにまたがって繋がった部分集合に、前記関連付元の部分集合に割り当てた固有情報から派生的に求められる固有情報を対応付けて、当該固有情報を、当該部分集合に含まれる各装置識別子に割り当てており、

前記端末装置は、

前記管理装置から予め配布された、関連付元の各部分集合に対応付けられた各固有情報のうち、当該端末装置の装置識別子を含む固有情報を記憶している固有情報記憶手段を

備えることを特徴とする端末装置。

[15] 前記固有情報記憶手段は、さらに、記憶している前記固有情報が対応付けられた部分集合を識別する集合識別情報を記憶しており、

前記端末装置は、さらに、

前記集合識別情報が、当該端末装置が有効な装置であることを示すか否かを判断する判断手段と、

前記判断手段による判断結果が肯定的である場合に、前記管理装置にて生成された各部分集合に対応付けられた各固有情報のうち特定の固有情報に基づく暗号化鍵により、メディア鍵が暗号化され、且つ前記暗号化鍵に関連する鍵関連情報と対応付けられた暗号化メディア鍵を取得する第1取得手段と、

前記固有情報記憶手段にて記憶している前記固有情報を用いて、前記暗号化鍵に対応する復号鍵を取得する第2取得手段と、

前記第2取得手段にて取得した前記復号鍵を用いて、前記取得手段にて取得した前記暗号化メディア鍵を復号して、前記メディア鍵を生成する復号手段とを備えることを特徴とする請求項14に記載の端末装置。

- [16] 前記特定の固有情報は、前記暗号化メディア鍵の生成時点で有効な端末装置の識別子を1以上含む部分集合に対応付けられた基準固有情報であり、
前記暗号化鍵は、共通鍵であり、
前記鍵関連情報は、前記基準固有情報が対応付けられた部分集合を識別する基準識別情報であり、
前記暗号化メディア鍵は、前記基準識別情報と対応付けられており、
前記判断手段は、前記固有情報記憶手段にて記憶している前記集合識別情報にて識別される部分集合から、前記基準識別情報にて識別される部分集合に至る経路が存在する場合に、前記集合識別情報は、当該端末装置が有効な装置であることを示す判断し、
前記第1取得手段は、前記基準識別情報に対応する前記基準固有情報に基づく暗号化鍵により暗号化された前記暗号化メディア鍵を取得し、
前記第2取得手段は、前記復号鍵を取得し、取得した前記復号鍵を前記共通鍵とし、
前記復号手段は、取得した前記共通鍵を用いて、前記暗号化メディア鍵を復号すること を特徴とする請求項15に記載の端末装置。
- [17] 前記管理装置は、前記最下位レイヤの部分集合をそっくり含み、且つ最小の要素数からなる部分集合を検索し、前記最下位レイヤの部分集合を親ノードとし、検索した部分集合を子ノードとして、関連付け、前記関連付先の部分集合をそっくり含み、最小の要素数からなり、且つ未関連付けである部分集合を検索し、前記関連付先の部分集合を親ノードとし、検索した部分集合を子ノードとして、関連付けて、前記最下位レイヤの部分集合をルートする部分集合木を生成し、
前記固有情報記憶手段は、さらに、前記管理装置にて生成された前記部分集合木を構成するデータ構造を予め記憶しており、
前記判断手段は、前記データ構造により構成される前記部分集合木を用いて、前

記固有情報記憶手段にて記憶している前記固有情報が対応付けられた部分集合から、前記基準識別情報にて識別される部分集合に至る経路が存在するか否かを判断する

ことを特徴とする請求項16に記載の端末装置。

- [18] 前記管理装置は、前記最下位レイヤの部分集合をそっくり含み、且つ最小の要素数からなる部分集合を検索し、前記最下位レイヤの部分集合を親ノードとし、検索した部分集合を子ノードとして、関連付け、前記関連付先の部分集合をそっくり含み、最小の要素数からなり、且つ未関連付けである部分集合を検索し、前記関連付先の部分集合を親ノードとし、検索した部分集合を子ノードとして、関連付けて、前記最下位レイヤの部分集合をルートする部分集合木を生成し、

前記基準識別情報は、前記基準固有情報に対応付けられた基準部分集合に対して、前記許可集合木のルートから、当該基準部分集合に至るまでの第1生成経路を含み、

前記集合識別情報は、前記固有情報に対応付けられた部分集合に対して、前記部分集合木のルートから、当該部分集合に至るまでの第2生成経路を含み、

前記判断手段は、前記第2生成経路が前記第1生成経路に含まれる場合に、前記集合識別情報にて識別される部分集合から、前記基準識別情報にて識別される部分集合に至る経路が存在すると判断する

ことを特徴とする請求項16に記載の端末装置。

- [19] 前記管理装置は、部分集合に対応付けられた固有情報を、一方向性関数に対する入力の情報として与え、前記固有情報に基づく共通鍵、及び前記固有情報から派生する固有情報を生成し、生成した固有情報を、入力の情報として与えた前記固有情報に対応付けられた部分集合と関連付けされた部分集合に対応付けて、関連付けされた部分集合に含まれる各装置識別子に、生成した固有情報を割り当て、

前記第2取得手段は、

前記一方向性関数と同一の関数を用いて、前記固有情報記憶手段にて記憶している前記固有情報から、前記固有情報に基づくデバイス鍵と、前記固有情報から派生する固有情報とを生成して、取得するデバイス鍵取得部と、

前記基準固有情報に基づくデバイス鍵を取得するまで、前記デバイス鍵取得部にて取得した前記固有情報を、前記関数に対する次の入力の情報として与えて、前記デバイス鍵取得部の動作を繰り返すよう制御する繰返部と、
前記デバイス鍵取得部にて取得した前記基準固有情報に基づくデバイス鍵を、前記共通鍵として取得する復号鍵取得手段と

を備えることを特徴とする請求項16に記載の端末装置。

[20] 前記端末装置は、さらに、

コンテンツを取得するコンテンツ取得手段と、

コンテンツ鍵を取得するコンテンツ鍵取得手段と、

前記コンテンツ鍵取得手段にて取得した前記コンテンツ鍵を、前記復号手段にて取得したメディア鍵を用いて、暗号化して暗号化コンテンツ鍵を生成する第1暗号化手段と、

前記コンテンツ取得手段にて取得した前記コンテンツを、前記コンテンツ鍵取得手段にて取得したコンテンツ鍵を用いて、暗号化して暗号化コンテンツを生成する第2暗号化手段と、

前記暗号化コンテンツ鍵と、前記暗号化コンテンツとを、記録媒体へ書き込む書込手段と

を備えることを特徴とする請求項19に記載の端末装置。

[21] 前記書込手段は、

前記暗号化コンテンツ鍵と、前記暗号化コンテンツとを、ネットワーク上に存在する装置が有する前記記録媒体へ、通信媒体を介して書き込む

ことを特徴とする請求項20に記載の端末装置。

[22] 前記端末装置は、さらに、

コンテンツ鍵が前記メディア鍵にて暗号化された暗号化コンテンツ鍵を取得する暗号化コンテンツ鍵取得手段と、

コンテンツが前記コンテンツ鍵にて暗号化された暗号化コンテンツを取得する暗号化コンテンツ取得手段と、

前記暗号化コンテンツ鍵取得手段にて取得した暗号化コンテンツ鍵を、前記メディ

ア鍵を用いて、復号して、前記コンテンツ鍵を生成する第1復号手段と、
前記暗号化コンテンツ取得手段にて取得した暗号化コンテンツを、前記コンテンツ鍵を用いて、復号して、前記コンテンツを生成する第2復号手段と、
前記第2復号にて生成された前記コンテンツを再生する再生手段と
を備えることを特徴とする請求項19に記載の端末装置。

- [23] 前記暗号化コンテンツ鍵及び前記暗号化コンテンツは、記録媒体に記録されており、前記記録媒体は、当該端末装置に装着され、
前記暗号化コンテンツ鍵取得手段は、前記記録媒体から、前記暗号化コンテンツ鍵を取得し、
前記暗号化コンテンツ取得手段は、前記記録媒体から、前記コンテンツを取得することを特徴とする請求項22に記載の端末装置。

- [24] 前記暗号化コンテンツ鍵取得手段は、通信媒体を介して、前記暗号化コンテンツ鍵を取得し、
前記暗号化コンテンツ取得手段は、通信媒体を介して、前記コンテンツを取得することを特徴とする請求項22に記載の端末装置。

- [25] 複数の端末装置と、前記複数の端末装置を識別する各装置識別子を木構造のリーフに配し、各装置識別子に、暗号化されたデータを復号する復号鍵の基となる固有情報を割り当て、管理する管理装置とからなる著作権保護システムであって、
前記管理装置は、
前記木構造のリーフを除く各レイヤのノードにおいて、その配下に存する装置識別子の部分集合を求めて、生成する部分集合生成手段と、
リーフのレイヤを除く最下位レイヤの部分集合をそっくり含む部分集合を直上位のレイヤから検索し、関連付ける第1関連付手段と、
関連付先の部分集合をそっくり含む部分集合を同一レイヤ及び直上位のレイヤの何れかから検索し、関連付ける第2関連付手段と、
最上位レイヤに至るまで、前記第2関連付手段が繰り返し処理するよう制御する第1制御手段と、
前記最下位レイヤの部分集合の全てに対して、前記第1関連付手段、前記第2関

連付手段、及び前記第1制御手段が繰り返し処理するよう制御する第2制御手段と、
前記最下位レイヤの関連付元の部分集合に、固有情報を対応付けて、当該固有情報を、当該部分集合に含まれる装置識別子に割り当てる第1割当手段と、

関連付けにより、レイヤにまたがって繋がった部分集合に、前記関連付元の部分集合に割り当てた固有情報から派生的に求められる固有情報を対応付けて、当該固有情報を、当該部分集合に含まれる各装置識別子に割り当てる第2割当手段と

を備えることを特徴とする著作権保護システム。

- [26] 前記第1関連付手段は、前記最下位レイヤの部分集合をそっくり含み、且つ最小の要素数からなる部分集合を検索し、前記最下位レイヤの部分集合を親ノードとし、検索した部分集合を子ノードとして、関連付け、

前記第2関連付手段は、前記関連付先の部分集合をそっくり含み、且つ最小の要素数からなる部分集合を検索し、前記関連付先の部分集合を親ノードとし、検索した部分集合を子ノードとして、関連付け、

前記第1制御手段は、最上位レイヤに至るまで、前記第2関連付手段が繰り返し処理するよう制御して、前記最下位レイヤの部分集合をルートする部分集合木を生成する

ことを特徴とする請求項25に記載の著作権保護システム。

- [27] 前記第1関連付手段は、前記最下位レイヤに対する各上位レイヤの各部分集合のうち、関連付けがなされた1以上の部分集合を除外し、残りの1以上の部分集合を用いて、最上位レイヤに至るまで、前記第2関連付手段が繰り返し処理するよう制御して、前記最下位レイヤの部分集合をルートする部分集合木を生成する

ことを特徴とする請求項26に記載の著作権保護システム。

- [28] 前記第2割当手段は、

前記派生的に求められる固有情報を、前記関連付元の部分集合に対応付けられた固有情報から一方向性関数を用いて生成し、生成した固有情報を、関連付けにより繋がった部分集合に対応付ける

ことを特徴とする請求項27に記載の著作権保護システム。

- [29] 前記管理装置は、さらに、

前記部分集合木のルートから1以上のリーフそれぞれに至る各経路において、固有情報を配布する配布対象の端末装置の識別子が、要素として初めて出現する部分集合が存在する場合に、前部分集合に対応付けされた固有情報を1以上取得する固有情報取得手段と、

取得した固有情報と、固有情報に対応する部分集合を識別する集合識別情報とからなる1以上の組を、前記配布対象の端末装置へ配布する配布手段と

を備えることを特徴とする請求項28に記載の著作権保護システム。

[30] 前記管理装置は、さらに、

前記部分集合木の構成要素である各部分集合と、前記各部分集合のそれぞれに対応付けされた前記固有情報とを記憶する領域を有する第1記憶手段と、

前記部分集合木を構成する複数のノードと、各ノードの子ノードとを記憶する領域を有する第2記憶手段と、

前記部分集合と、前記部分集合に対応付けされた固有情報とを対応付けて、前記第1記憶手段に書き込む第1書込手段と、

前記部分集合木を構成する前記ノードと、前記ノードの子ノードとを対応付けて、前記第2記憶手段に書き込む第2書込手段と

を備えることを特徴とする請求項29に記載の著作権保護システム。

[31] 前記第2制御手段は、前記最下位レイヤの部分集合の全てに対して、前記第1関連付手段、前記第2関連付手段、及び前記第1制御手段が繰り返し処理するよう制御して、複数の部分集合木を生成し、

前記第1記憶手段は、各部分集合木に含まれる各部分集合と、前記各部分集合のそれぞれに対応付けされた各固有情報とを記憶しており、

前記管理装置は、さらに、

前記複数の端末装置のうち、1以上の無効な端末を示す無効な識別子を記憶する領域を有する無効化識別子記憶手段と、

前記無効化識別子記憶手段にて記憶されている内容に基づいて、前記第1記憶手段より1以上の部分集合を取得し、取得した各部分集合のそれぞれに対応付けされた各固有情報に基づいて、1以上の暗号化鍵を取得し、取得した各暗号化鍵を個

別に用いて、コンテンツの利用に用いるメディア鍵を暗号し、前記1以上の暗号化鍵と同数の暗号化メディア鍵を生成する暗号化鍵生成手段と、

前記暗号化メディア鍵と、前記暗号化メディア鍵に対する暗号化鍵の取得に用いられた部分集合を識別する基準識別情報とからなる1以上の組を、当該管理装置に装着された記録媒体へ書き込む第3書込手段と

を備えることを特徴とする請求項30に記載の著作権保護システム。

[32] 前記管理装置は、さらに、

無効な識別子を受け取り、受け取った無効な識別子を前記無効化識別子記憶手段へ書き込む無効化識別子受取手段

を備えることを請求項31に記載の著作権保護システム。

[33] 前記暗号化鍵は、前記復号鍵と同一の共通鍵であり、

前記一方向性関数は、さらに、各固有情報から前記各固有情報に基づく各共通鍵を生成し、

前記暗号化鍵生成手段は、

前記無効化識別子記憶手段にて記憶されている無効な識別子を除く1以上の有効な識別子を最も多く含む部分集合を、前記第1記憶手段より取得する部分集合取得部と、

全ての有効な識別子が、前記部分集合取得部にて取得される1以上の部分集合の何れかに属するまで、前記部分集合取得部が繰り返し処理するよう制御する制御部と、

前記一方向性関数を用いて、前記部分集合取得部にて取得した各部分集合のそれぞれに対応付けされた各固有情報から生成された1以上の共通鍵を取得する共通鍵取得部と、

前記共通鍵取得部にて取得した各共通鍵を用いて、共通鍵の数と同数の暗号化メディア鍵を生成する暗号化部と

を備えることを特徴とする請求項31に記載の著作権保護システム。

[34] 前記端末装置は、

前記管理装置の配布手段にて予め配布された固有情報と、前記固有情報が対

応付けされた部分集合を識別する集合識別情報とからなる1以上の組を記憶している固有情報記憶手段と、

前記集合識別情報が、当該端末装置が有効な装置であることを示すか否かを判断する判断手段と、

前記判断手段による判断結果が肯定的である場合に、前記記録媒体から暗号化メディア鍵を1個取得する第1取得手段と、

前記固有情報記憶手段にて記憶している前記固有情報を用いて、前記暗号化鍵に対応する復号鍵を取得する第2取得手段と、

前記第2取得手段にて取得した前記復号鍵を用いて、前記取得手段にて取得した前記暗号化メディア鍵を復号して、前記メディア鍵を生成する復号手段と

を備えることを特徴とする請求項33に記載の著作権保護システム。

[35] 前記暗号化鍵は、共通鍵であり、

前記判断手段は、前記固有情報記憶手段にて記憶している前記集合識別情報にて識別される部分集合から、前記基準識別情報にて識別される部分集合に至る経路が存在する場合に、前記集合識別情報は、当該端末装置が有効な装置であることを示す判断し、

前記第1取得手段は、前記基準識別情報に対応する暗号化メディア鍵を取得し、

前記第2取得手段は、前記復号鍵を取得し、取得した前記復号鍵を前記共通鍵とし、

前記復号手段は、取得した前記共通鍵を用いて、前記暗号化メディア鍵を復号することを特徴とする請求項34に記載の著作権保護システム。

[36] 前記第2取得手段は、

前記一方向性関数と同一の関数を用いて、前記固有情報記憶手段にて記憶している前記固有情報から、前記固有情報に基づくデバイス鍵と、前記固有情報から派生する固有情報とを生成して、取得するデバイス鍵取得部と、

前記基準固有情報に基づくデバイス鍵を取得するまで、前記デバイス鍵取得部にて取得した前記固有情報を、前記関数に対する次の入力の情報として与えて、前記デバイス鍵取得部の動作を繰り返すよう制御する繰返部と、

前記デバイス鍵取得部にて取得した前記基準固有情報に基づくデバイス鍵を、前記共通鍵として取得する復号鍵取得手段と

を備えることを特徴とする請求項35に記載の著作権保護システム。

[37] 記録媒体であって、

有効な端末装置により生成される復号鍵に対応し、且つ1以上の有効な端末装置からなる集合に対応する固有情報に基づいて生成された暗号化鍵を用いて、メディア鍵が暗号化された暗号化メディア鍵を記憶している暗号化鍵記憶手段を備えることを特徴とする記録媒体。

[38] 前記暗号化鍵記憶手段は、さらに、

前記暗号化鍵の生成に用いた固有情報に対応する集合を識別する集合識別情報を記憶している

ことを特徴とする請求項37に記載の記録媒体。

[39] 複数の端末装置を識別する各装置識別子を木構造のリーフに配し、各装置識別子に、暗号化されたデータを復号する復号鍵の基となる固有情報を割り当て、管理する管理装置であって、

前記木構造のリーフを除く各レイヤのノードにおいて、その配下に存する装置識別子の部分集合を求めて、生成する部分集合生成手段と、

同一レイヤにおいて存在する部分集合のうち、最小の要素数の部分集合を含む他の部分集合を、最小の要素数の部分集合とともに1つのグループにまとめるグループ生成手段と、

同一レイヤの存在する最小の要素数の部分集合の全てに対して、前記グループ生成手段が繰り返し処理するよう制御する第1制御手段と、

全てのレイヤに対して、前記グループ生成手段及び前記第1制御手段が繰り返し処理するよう制御する第2制御手段と、

前記第2制御手段にて全てのレイヤに対して、処理を行った後、異なるレイヤ間において、下位レイヤのグループの何れかの部分集合を全て含む部分集合を有する上位レイヤのグループを、当該下位レイヤのグループと1のグループに統合する統合手段と、

全てのレイヤにおいてグループの統合後に、残存する各グループ内の最小の要素数の各部分集合に対して、各固有情報を対応付けて、各部分集合に含まれる1以上の装置識別子に、対応付けられた各固有情報を割り当てる第1割当手段と、

前記第1割当手段にて各固有情報を割り当てた最小の要素数の各部分集合と異なる各部分集合に対して、部分集合が属するグループに存在する最小の要素数の部分集合に対応付けされた固有情報から派生的に求められる固有情報を対応付けて、各部分集合に含まれる1以上の装置識別子に、対応付けられた固有情報を割り当てる第2割当手段と

を備えることを特徴とする管理装置。

[40] 複数の端末装置を識別する各装置識別子を木構造のリーフに配し、各装置識別子に、暗号化されたデータを復号する復号鍵の基となる固有情報を割り当て、管理する管理装置に用いられる関連付方法であって、

前記木構造のリーフを除く各レイヤのノードにおいて、その配下に存する装置識別子の部分集合を求めて、生成する部分集合生成ステップと、

リーフのレイヤを除く最下位レイヤの部分集合をそっくり含む部分集合を直上位のレイヤから検索し、関連付ける第1関連付ステップと、

関連付先の部分集合をそっくり含む部分集合を同一レイヤ及び直上位のレイヤの何れかから検索し、関連付ける第2関連付ステップと、

最上位レイヤに至るまで、前記第2関連付手段が繰り返し処理するよう制御する第1制御ステップと、

前記最下位レイヤの部分集合の全てに対して、前記第1関連付手段、前記第2関連付手段、及び前記第1制御手段が繰り返し処理するよう制御する第2制御ステップと、

前記最下位レイヤの関連付元の部分集合に、固有情報を対応付けて、当該固有情報を、当該部分集合に含まれる装置識別子に割り当てる第1割当ステップと、

関連付けにより、レイヤにまたがって繋がった部分集合に、前記関連付元の部分集合に割り当てた固有情報から派生的に求められる固有情報を対応付けて、当該固有情報を、当該部分集合に含まれる各装置識別子に割り当てる第2割当ステップと

を含むことを特徴とする関連付方法。

- [41] 複数の端末装置を識別する各装置識別子を木構造のリーフに配し、各装置識別子に、暗号化されたデータを復号する復号鍵の基となる固有情報を割り当て、管理する管理装置に、

前記木構造のリーフを除く各レイヤのノードにおいて、その配下に存する装置識別子の部分集合を求めて、生成する部分集合生成ステップと、

リーフのレイヤを除く最下位レイヤの部分集合をそっくり含む部分集合を直上位のレイヤから検索し、関連付ける第1関連付ステップと、

関連付先の部分集合をそっくり含む部分集合を同一レイヤ及び直上位のレイヤの何れかから検索し、関連付ける第2関連付ステップと、

最上位レイヤに至るまで、前記第2関連付手段が繰り返し処理するよう制御する第1制御ステップと、

前記最下位レイヤの部分集合の全てに対して、前記第1関連付手段、前記第2関連付手段、及び前記第1制御手段が繰り返し処理するよう制御する第2制御ステップと、

前記最下位レイヤの関連付元の部分集合に、固有情報を対応付けて、当該固有情報を、当該部分集合に含まれる装置識別子に割り当てる第1割当ステップと、

関連付けにより、レイヤにまたがって繋がった部分集合に、前記関連付元の部分集合に割り当てた固有情報から派生的に求められる固有情報を対応付けて、当該固有情報を、当該部分集合に含まれる各装置識別子に割り当てる第2割当ステップと

を実行させるための関連付プログラム。

- [42] 複数の端末装置を識別する各装置識別子を木構造のリーフに配し、各装置識別子に、暗号化されたデータを復号する復号鍵の基となる固有情報を割り当て、管理する管理装置に、

前記木構造のリーフを除く各レイヤのノードにおいて、その配下に存する装置識別子の部分集合を求めて、生成する部分集合生成ステップと、

リーフのレイヤを除く最下位レイヤの部分集合をそっくり含む部分集合を直上位のレイヤから検索し、関連付ける第1関連付ステップと、

関連付先の部分集合をそっくり含む部分集合を同一レイヤ及び直上位のレイヤの何れかから検索し、関連付ける第2関連付ステップと、

最上位レイヤに至るまで、前記第2関連付手段が繰り返し処理するよう制御する第1制御ステップと、

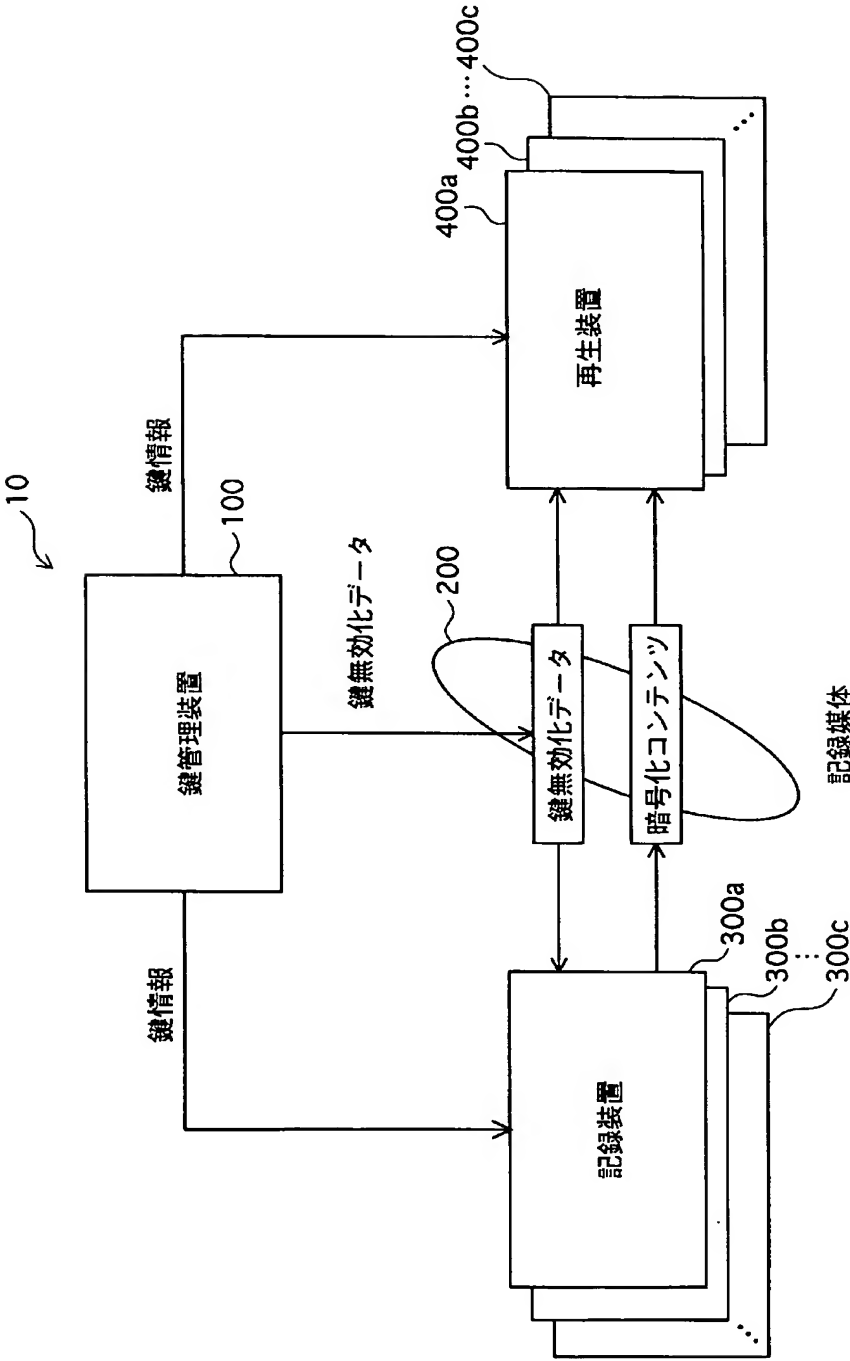
前記最下位レイヤの部分集合の全てに対して、前記第1関連付手段、前記第2関連付手段、及び前記第1制御手段が繰り返し処理するよう制御する第2制御ステップと、

前記最下位レイヤの関連付元の部分集合に、固有情報を対応付けて、当該固有情報を、当該部分集合に含まれる装置識別子に割り当てる第1割当ステップと、

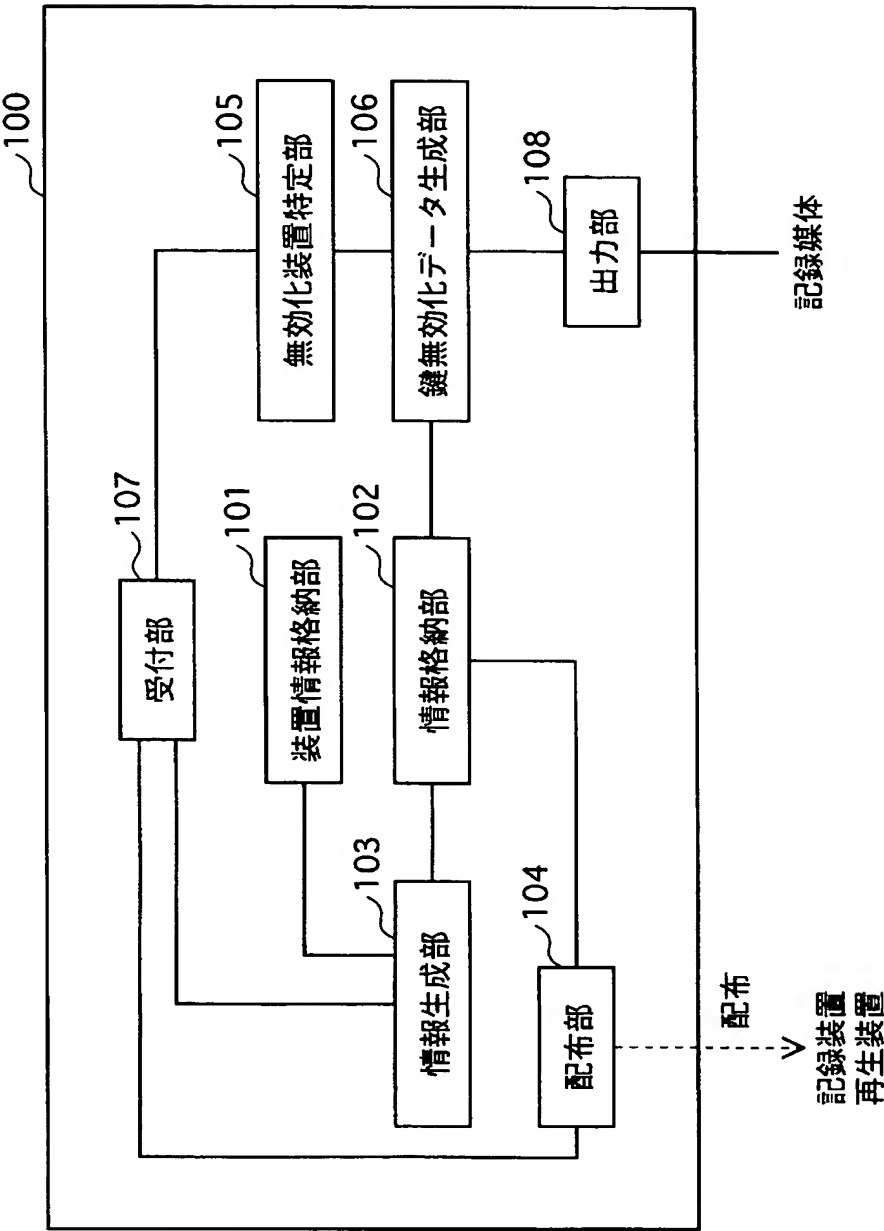
関連付けにより、レイヤにまたがって繋がった部分集合に、前記関連付元の部分集合に割り当てた固有情報から派生的に求められる固有情報を対応付けて、当該固有情報を、当該部分集合に含まれる各装置識別子に割り当てる第2割当ステップと

を実行させるための関連付プログラムを記録したコンピュータ読み取り可能なプログラム記録媒体。

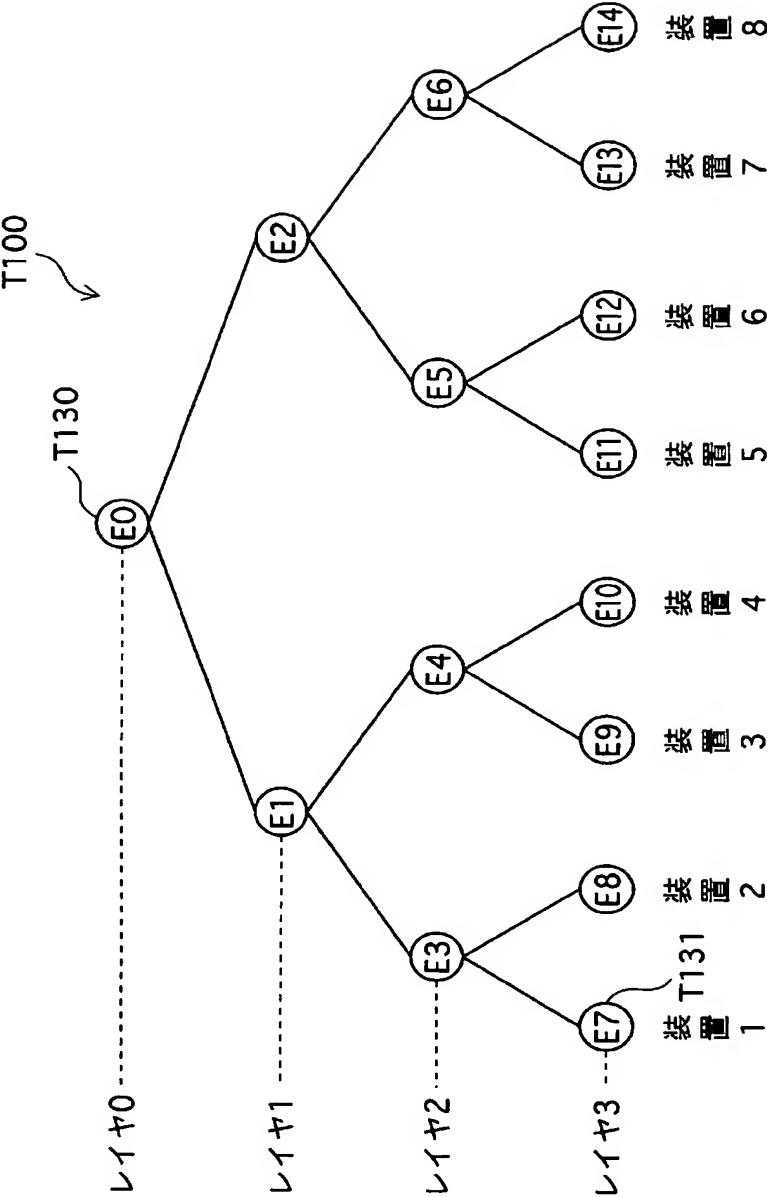
[図1]



[図2]



[図3]



[図4]

T171	T172	T173	T101
親ノード名	子ノード名	装置識別子	
E0	E1		
E0	E2	—	
E1	E3	—	
E1	E4	—	
E2	E5	—	
E2	E6	—	
E3	E7	—	
E3	E8	—	
E4	E9	—	
E4	E10	—	
E5	E11	—	
E5	E12	—	
E6	E13	—	
E6	E14	—	
E7	—	装置1	
E8	—	装置2	
E9	—	装置3	
E10	—	装置4	
E11	—	装置5	
E12	—	装置6	
E13	—	装置7	
E14	—	装置8	

[5]

D201 D202 D203	1234567 A1RLRL K8	1234568 A1RLRL K9	1234578 A1RLRL K10	1234678 A1RLRR K11	1235678 A5RLRL K25	1245678 A5RLRL K26	1345678 A5RLRL K27	2345678 A5RLRR K28
	123456 A1RLRL K6	123478 A1RLRR K7	125678 A5RLRL K23	345678 A5RLRR K24				
	1234 A1RLR K5	5678 A5RLR K22						
	123 A1RL K3	124 A1RR K4	134 A3RL K15	234 A3RR K16	567 A5RL K20	568 A5RR K21	578 A7RL K32	678 A7RR K33
	12 A1R K2	34 A3R K14	56 A5R K19	78 A7R K31				
	1 A1 K1	2 A2 K12	3 A3 K13	4 A4 K17	5 A5 K18	6 A6 K29	7 A7 K30	8 A8 K34

D100

D200 D204

[図6]

D101

	親ノード	子ノード	ルート情報
D301	1	12	ルート
	12	123	
	12	124	
	123	1234	
D302	124	—	
	1234	123456	
	1234	123478	
	123456	1234567	
	123456	1234568	
	123478	1234578	
	123478	1234678	
D303	1234567	—	
	1234568	—	
	1234578	—	
	1234678	—	
D311	2	—	ルート
	3	34	ルート
	34	134	
	34	234	
D321	134	—	
D322	234	—	
D331	4	—	ルート
	5	56	ルート
	56	567	
	56	568	
	567	5678	
	568	—	
	5678	125678	
	5678	345678	
	125678	1235678	
	125678	1245678	
	345678	1345678	
	345678	2345678	
	1235678	—	
	1245678	—	
	1345678	—	
	2345678	—	
	6	—	ルート
	7	78	ルート
	78	578	
	78	678	
	578	—	
	678	—	
	8	—	ルート

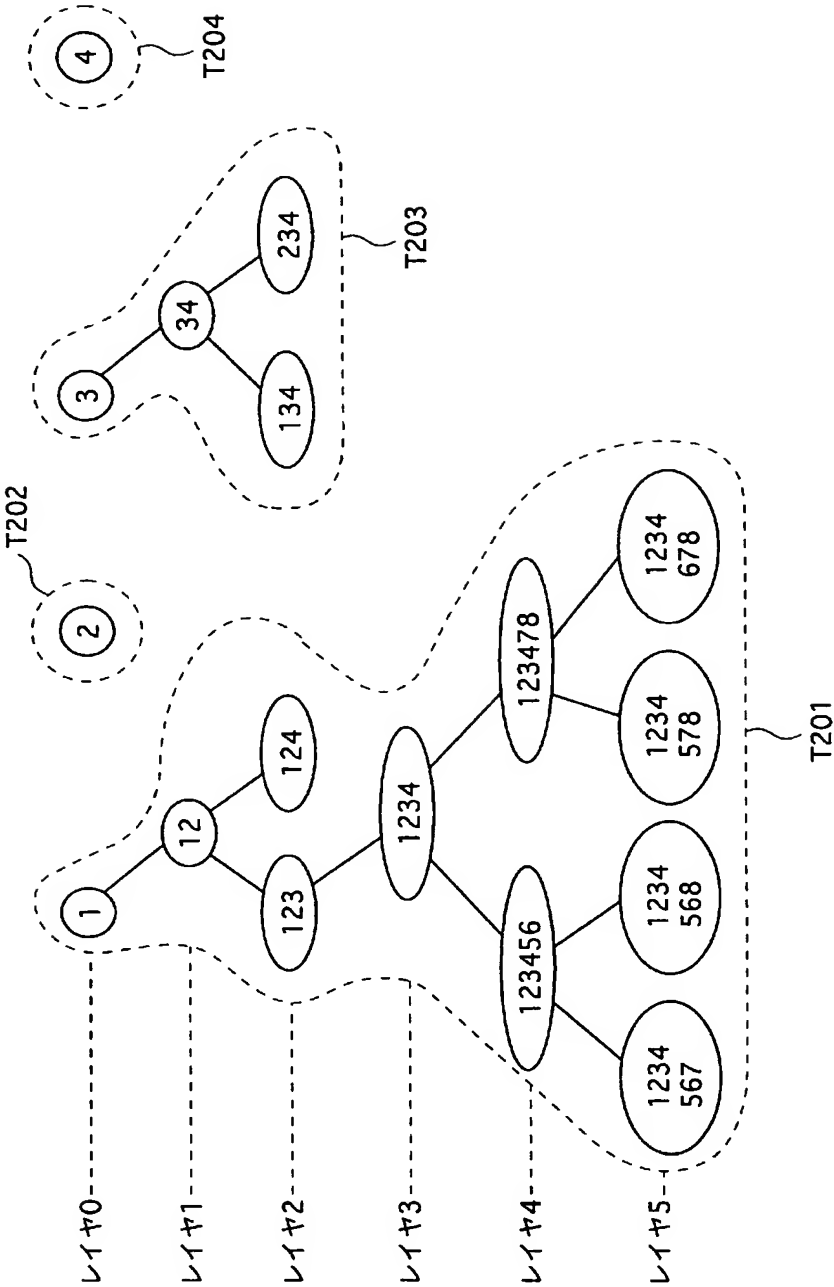
D300

D310

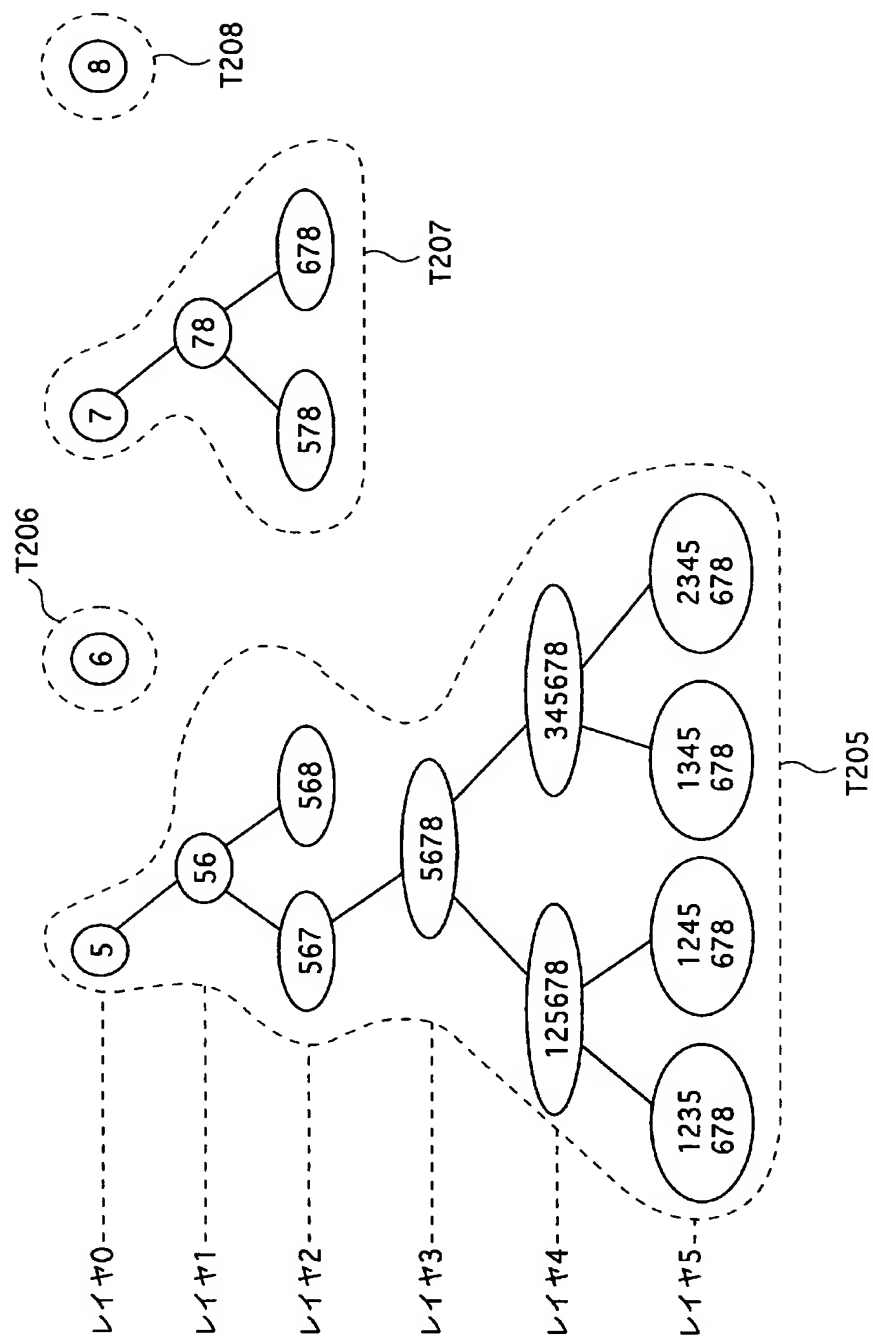
D320

D330

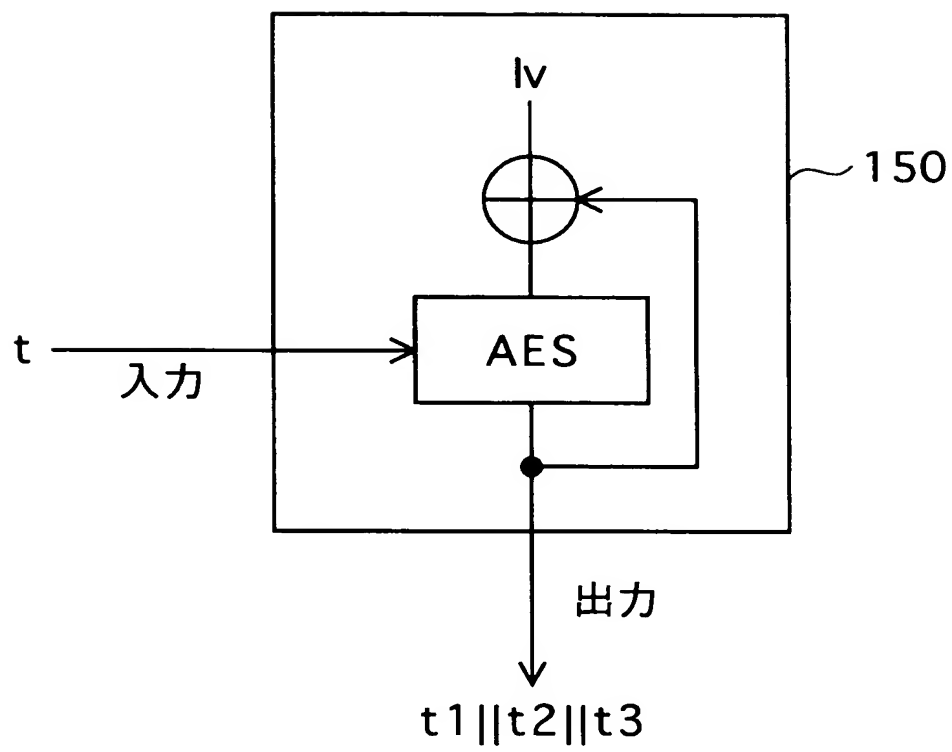
[図7]



[図8]



[図9]

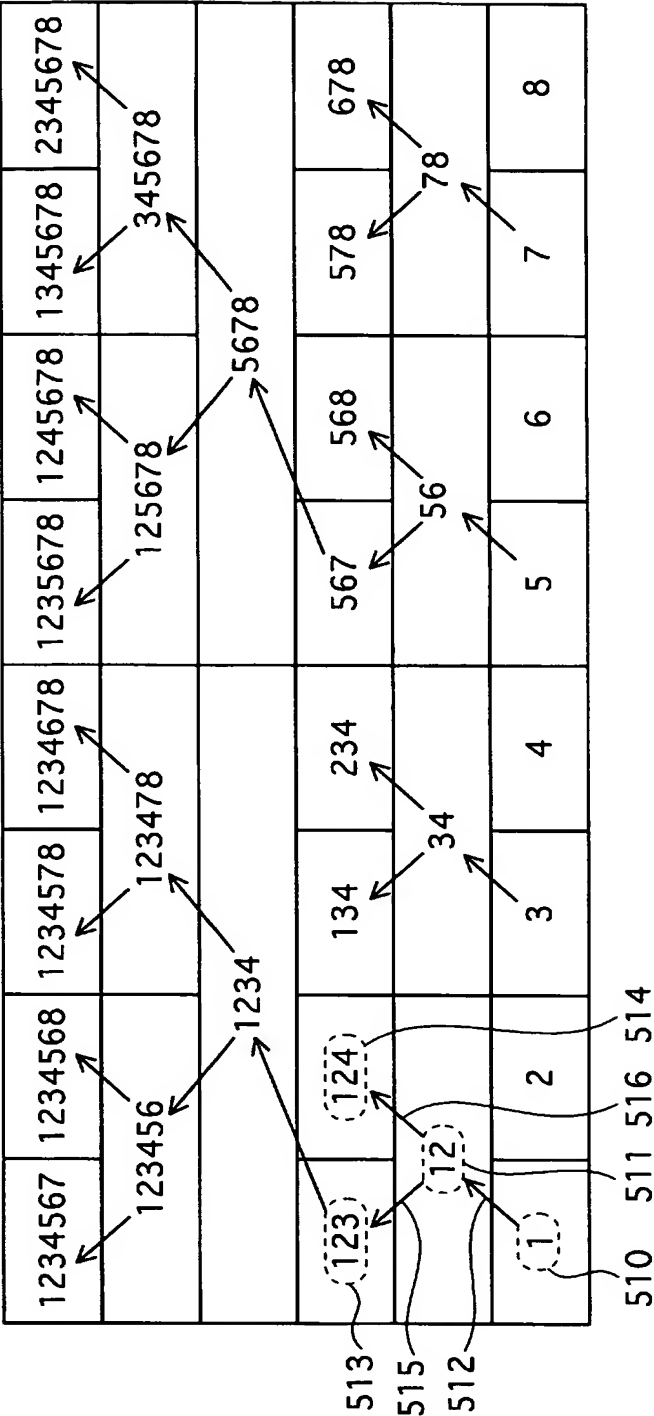


[図10]

D100a

501	1234567	1234568	1234578	1234678	1235678	1245678	1345678	2345678
502	123456	123478	125678	345678				
503	1234	5678						
504	123	124	134	234	567	568	578	678
505	12	34	56	78				
506	1	2	3	4	5	6	7	8

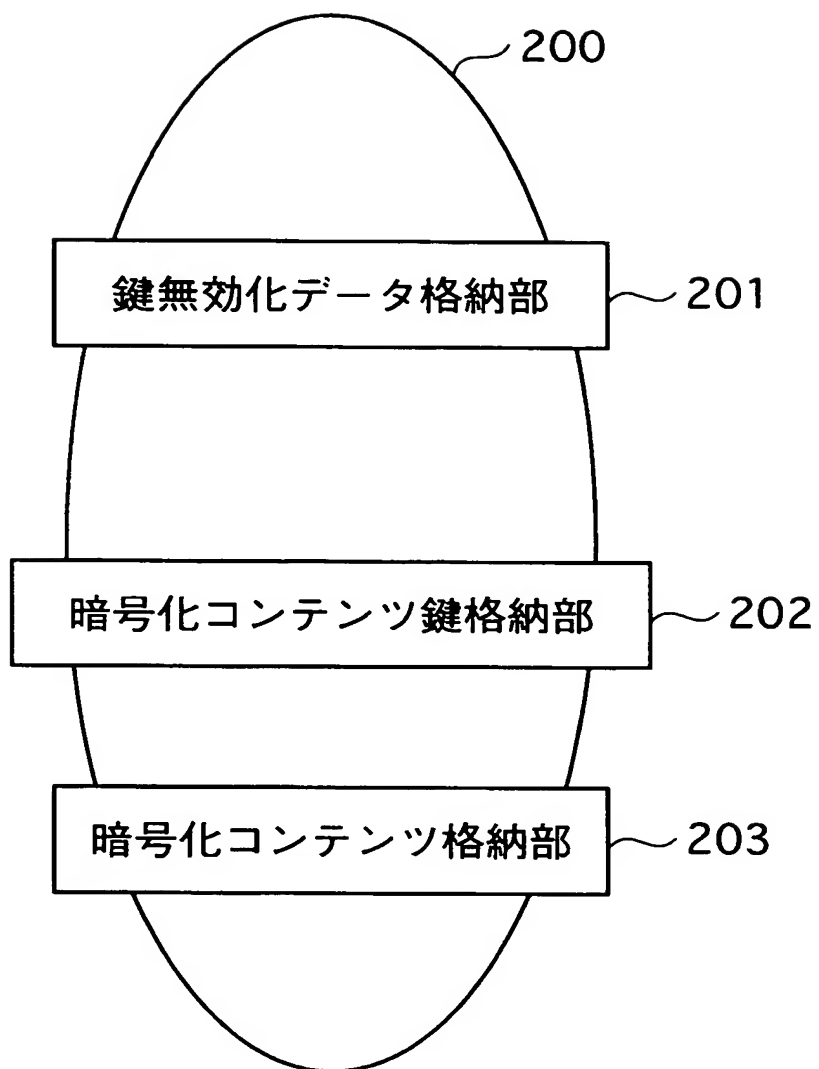
[図11]



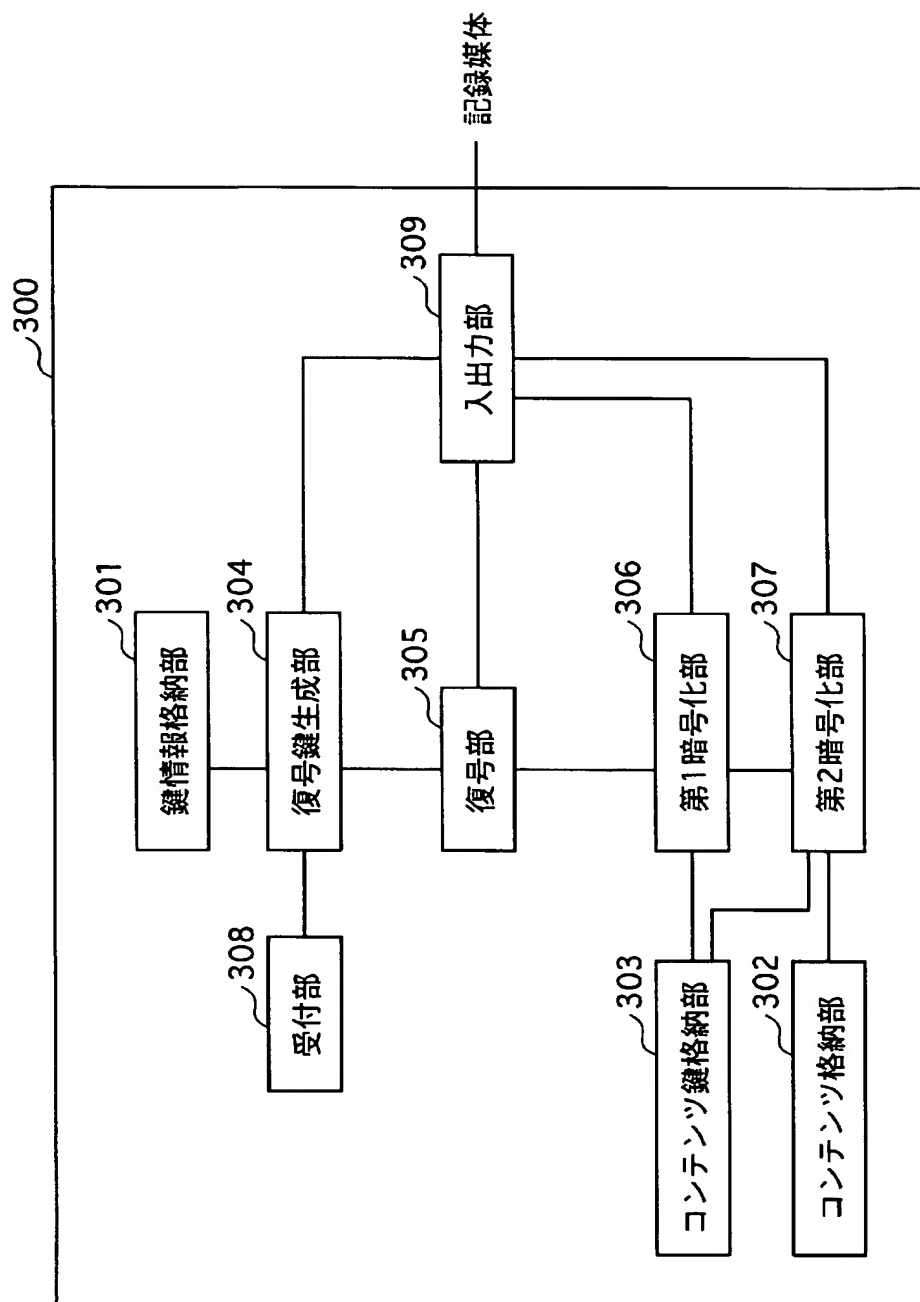
[図12]

装置名	合計	521	520	522	523	524	525	526	527	D400
装置が保持する鍵情報										
装置1	4個 (-2)	1 A1	(134) A3RL	(125678) A5RLRL	(1345678) A5RLRRL					
装置2	5個 (-1)	2 A2	12 A1R	234 A3RR	125678 A5RLRL	2345678 A5RLRRR				
装置3	4個 (-2)	3 A3	123 A1RL	345678 A5RLRR	1235678 A5RLRLL					
装置4	6個 (0)	4 A4	34 A3R	124 A1RR	1234 A1RLR	345678 A5RLRR	1245678 A5RLRLR			
装置5	4個 (-2)	5 A5	578 A7RL	123456 A1RLRL	1234578 A1RLRRL					
装置6	5個 (-1)	6 A6	56 A5R	678 A7RR	123456 A1RLRL	1234678 A1RLRRR				
装置7	4個 (-2)	7 A7	567 A5RL	123478 A1RLRR	1234567 A1RLRLL					
装置8	6個 (0)	8 A8	78 A7R	568 A5RR	5678 A5RLR	123478 A1RLRR	1234568 A1RLRLR			

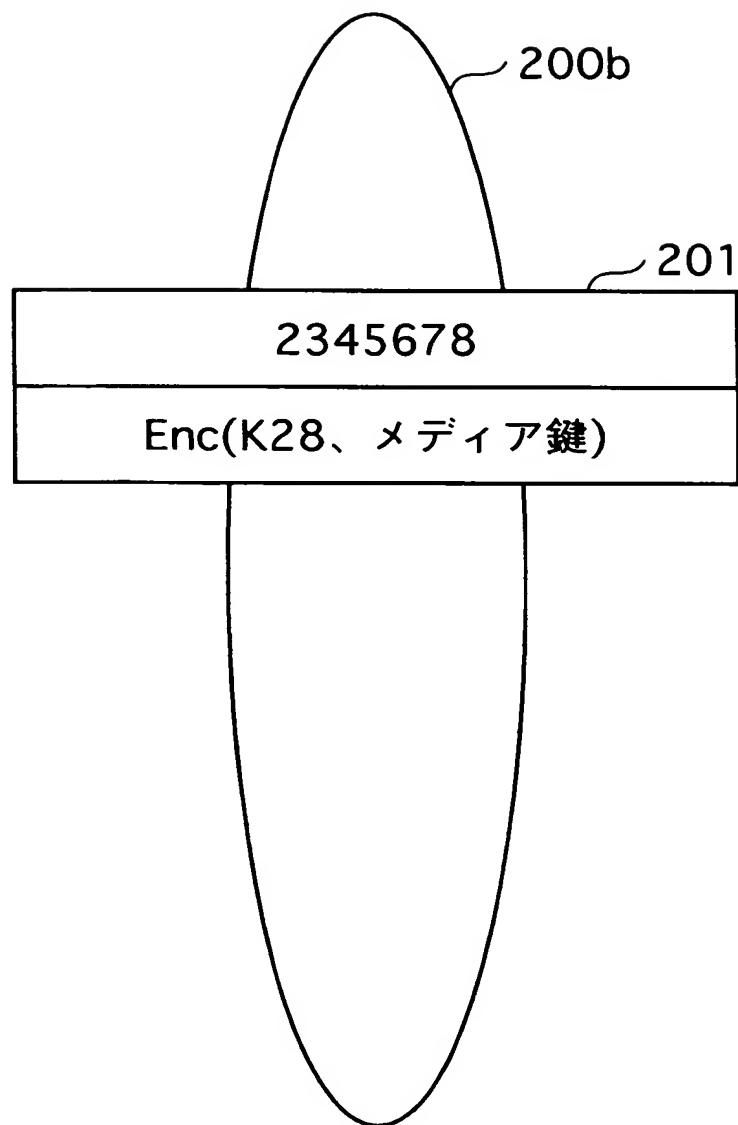
[図13]



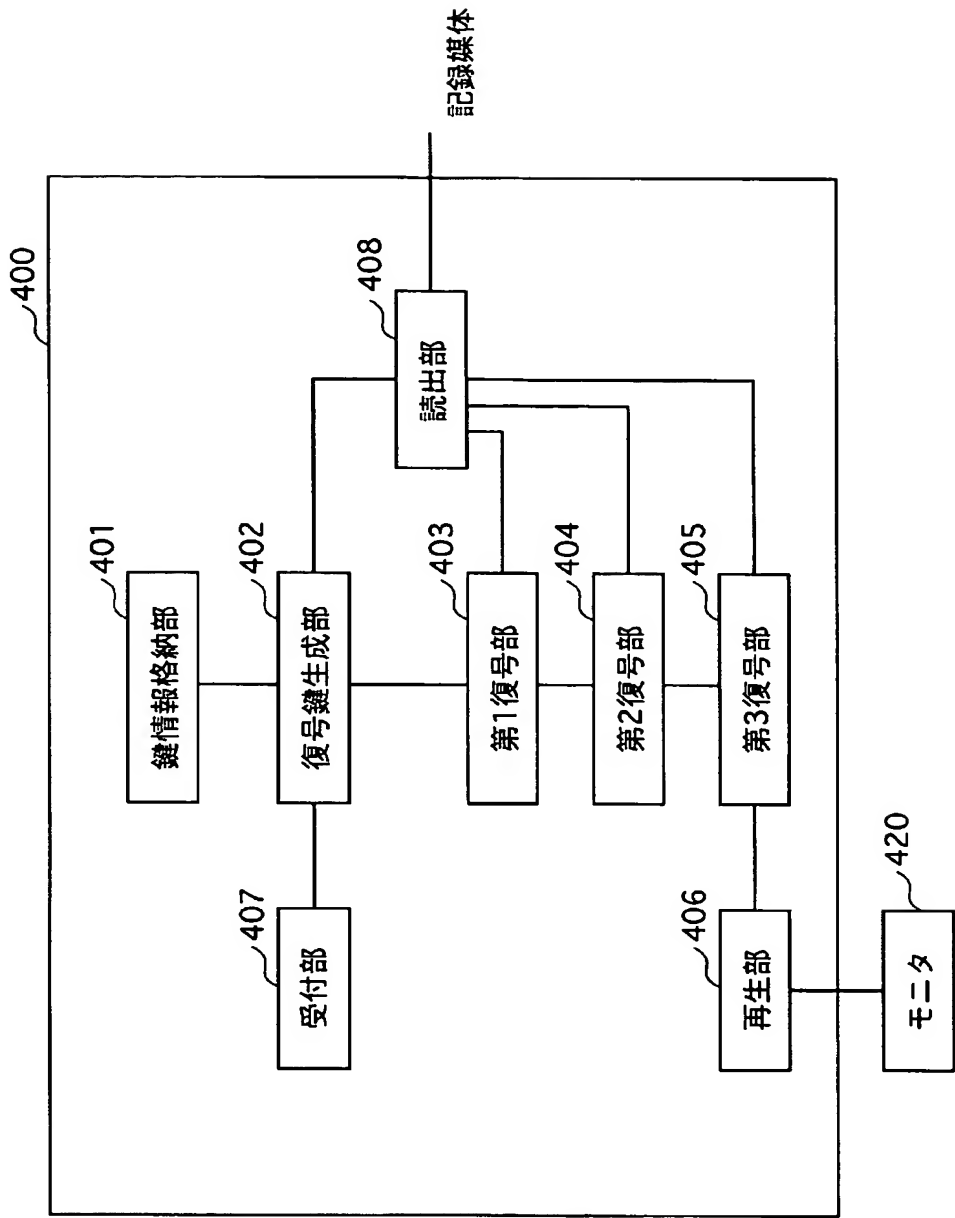
[図14]



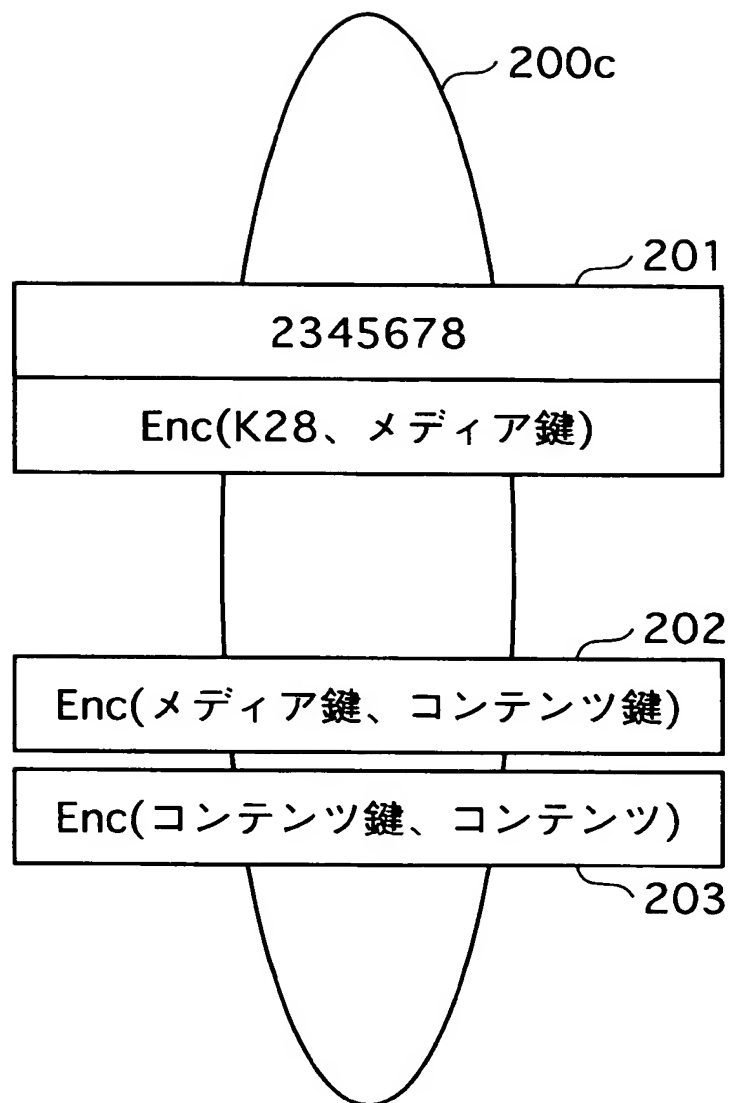
[図15]



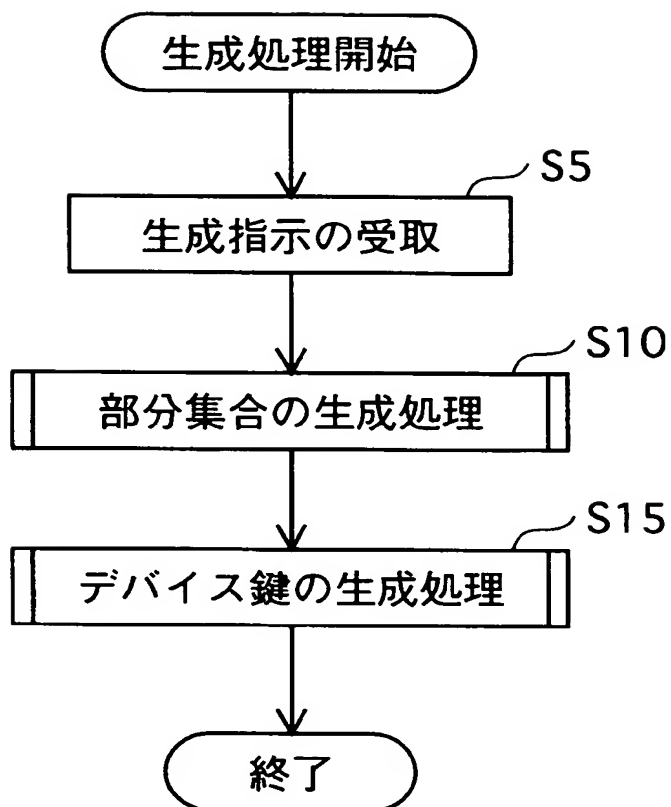
[図16]



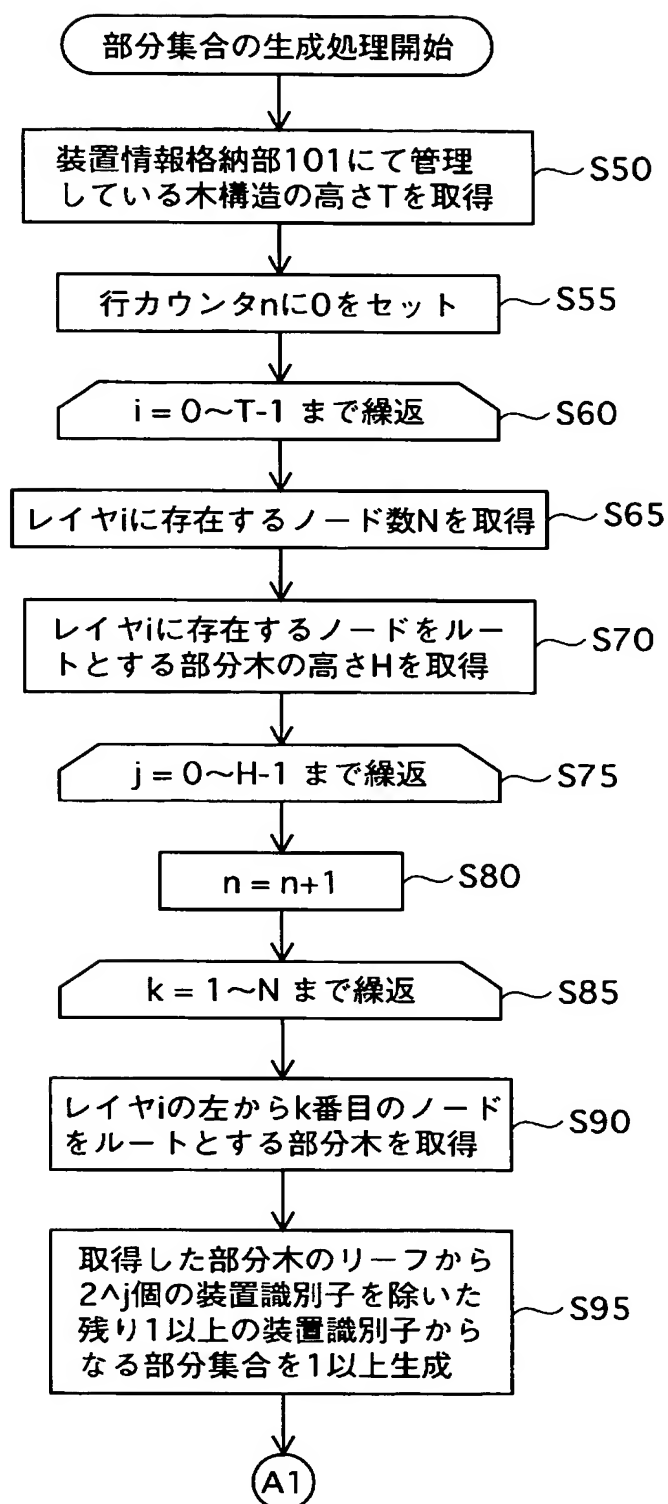
[図17]



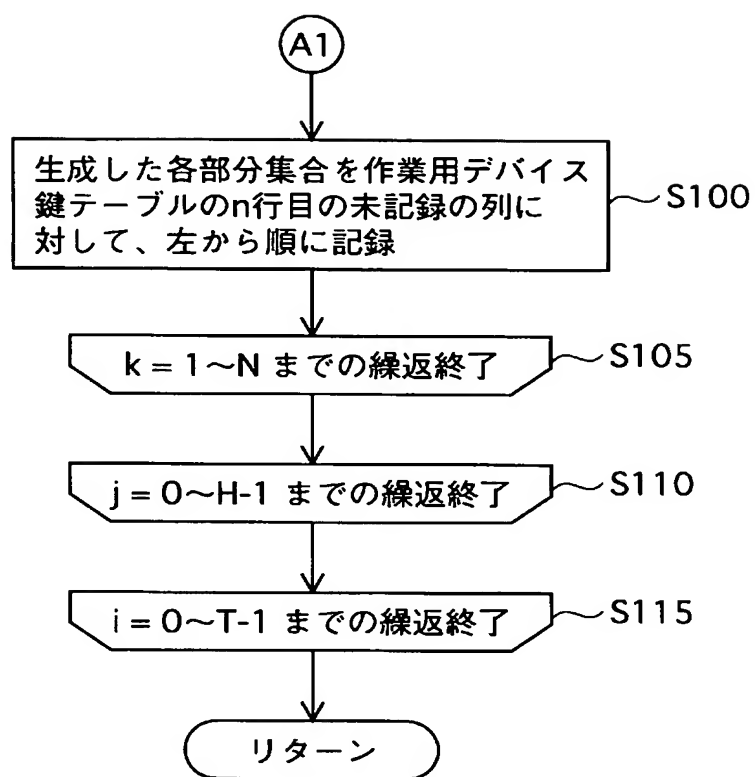
[図18]



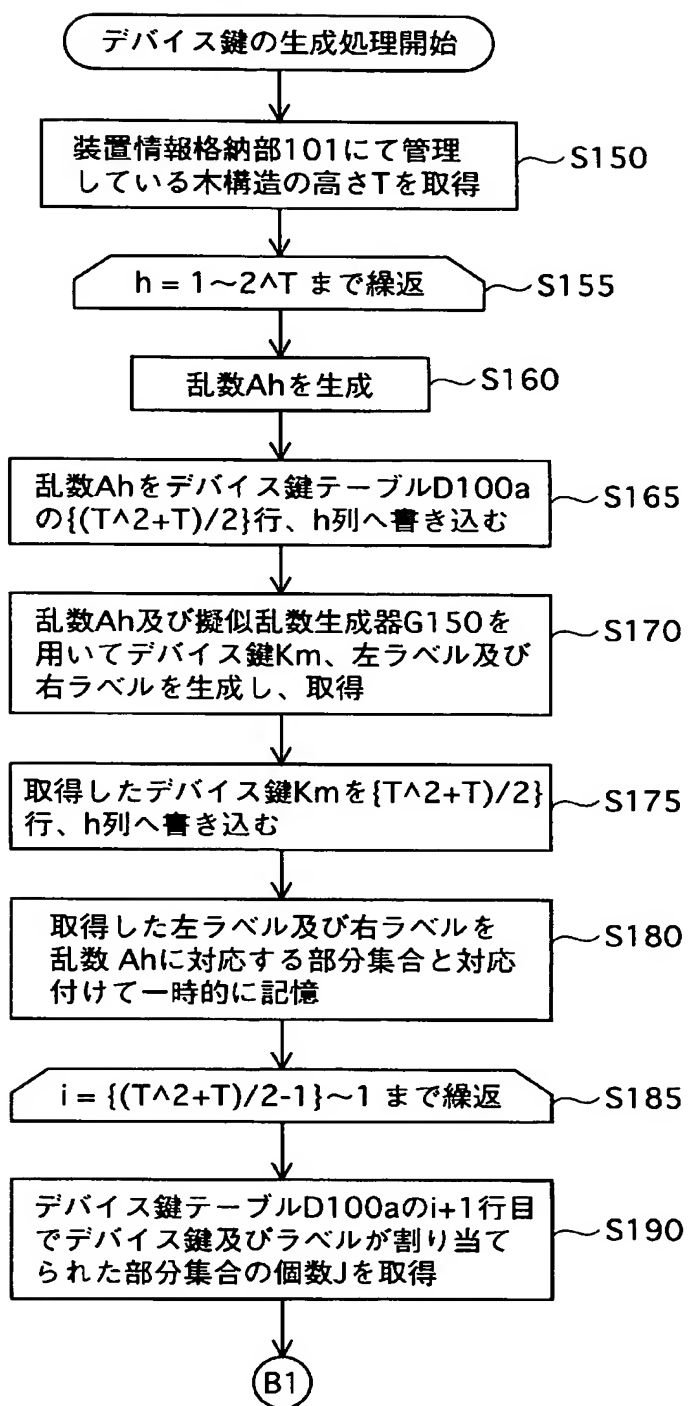
[図19]



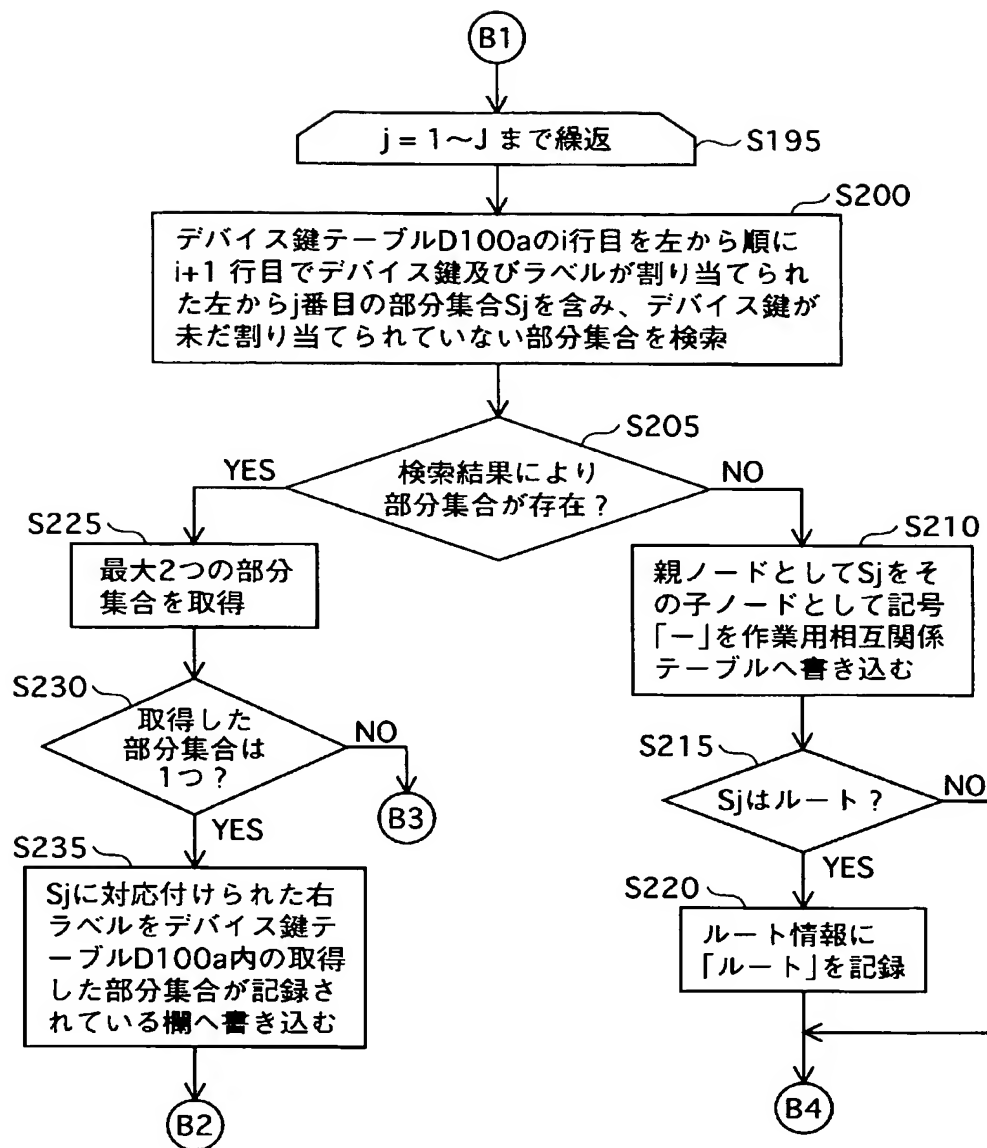
[図20]



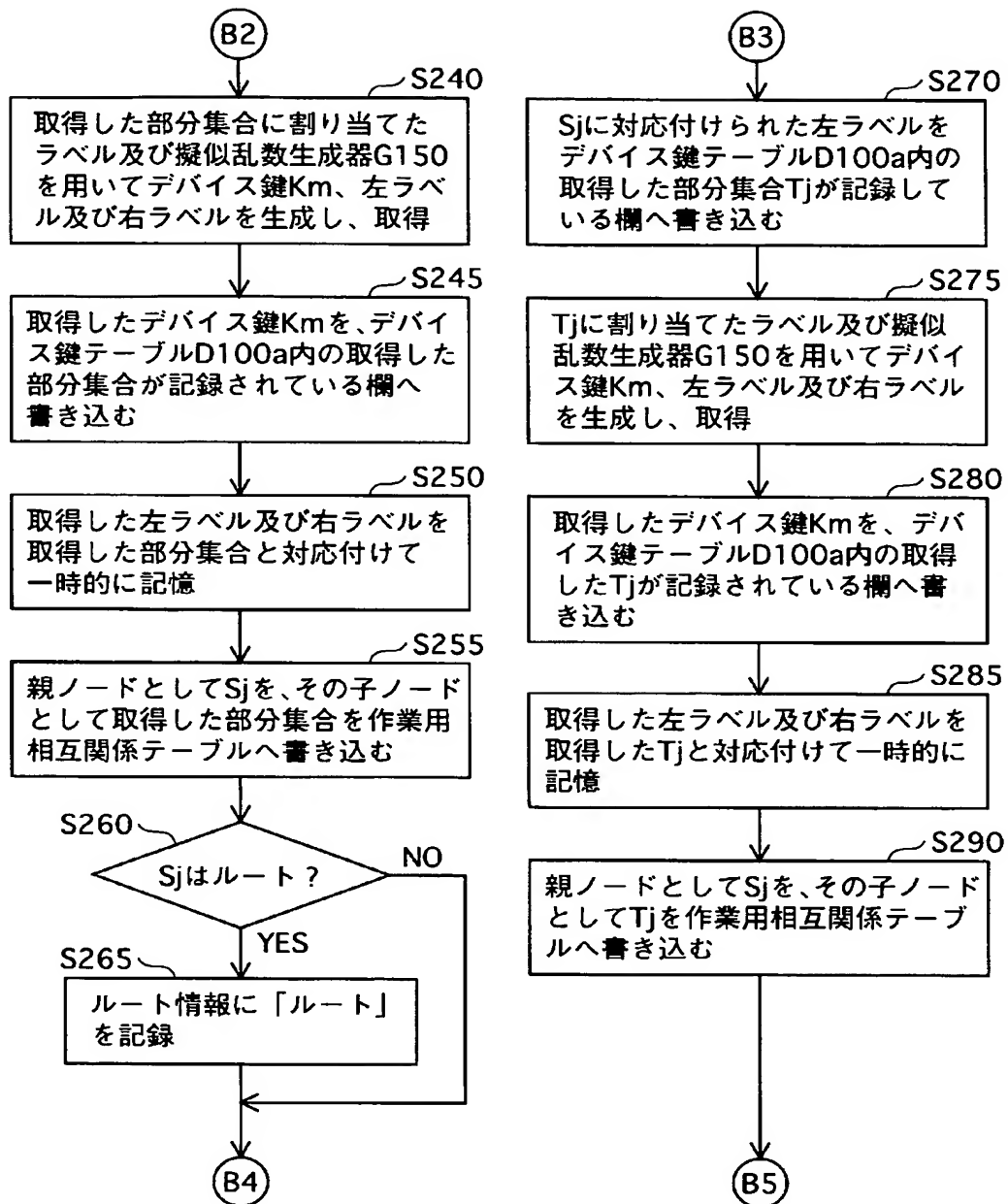
[図21]



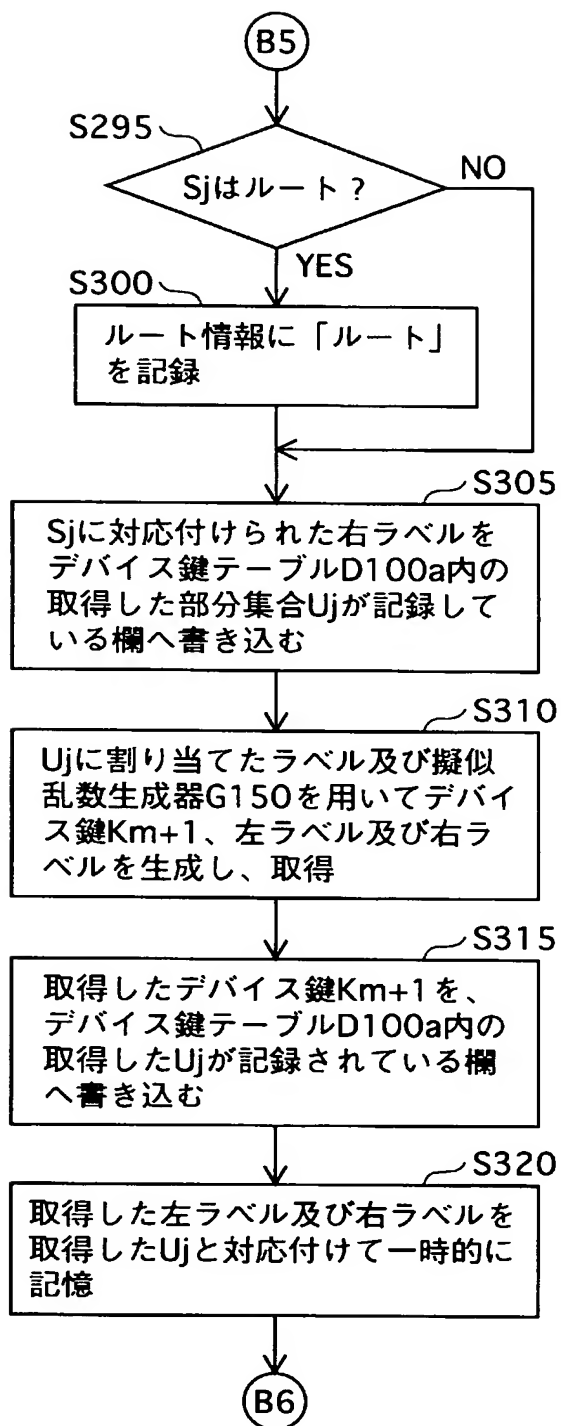
[図22]



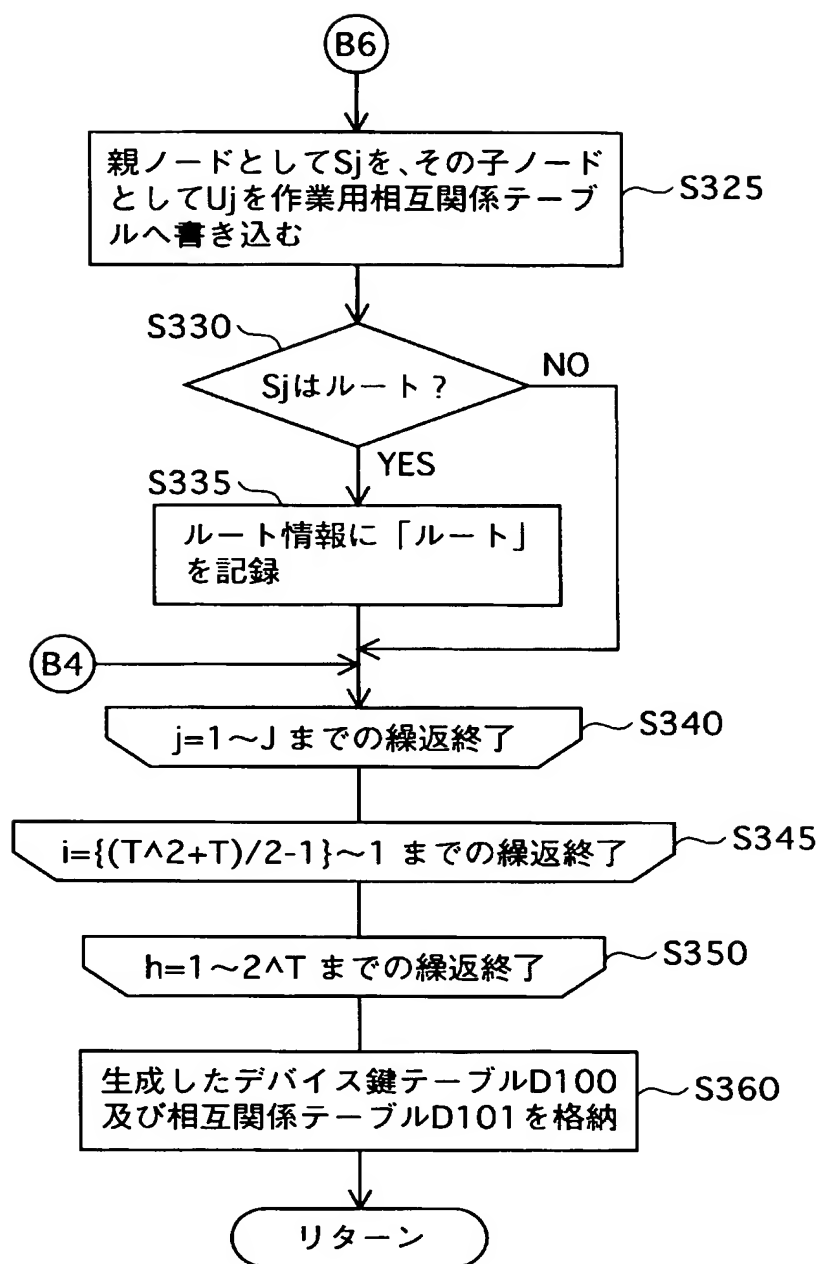
[図23]



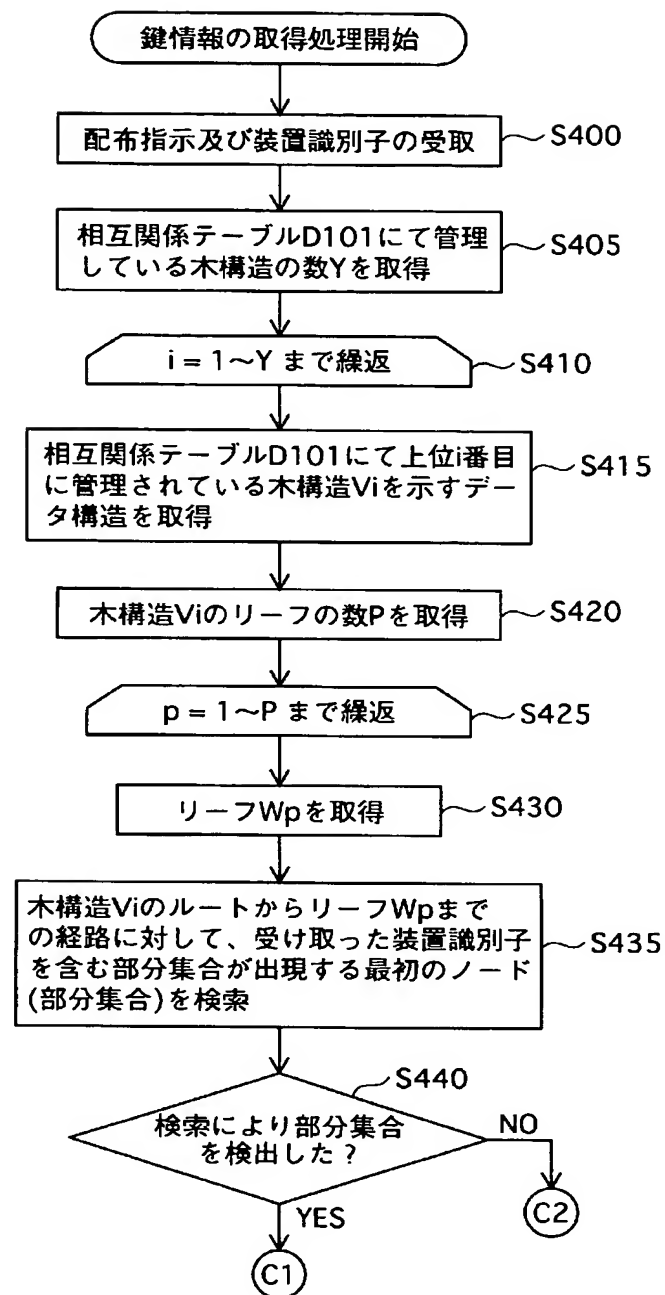
[図24]



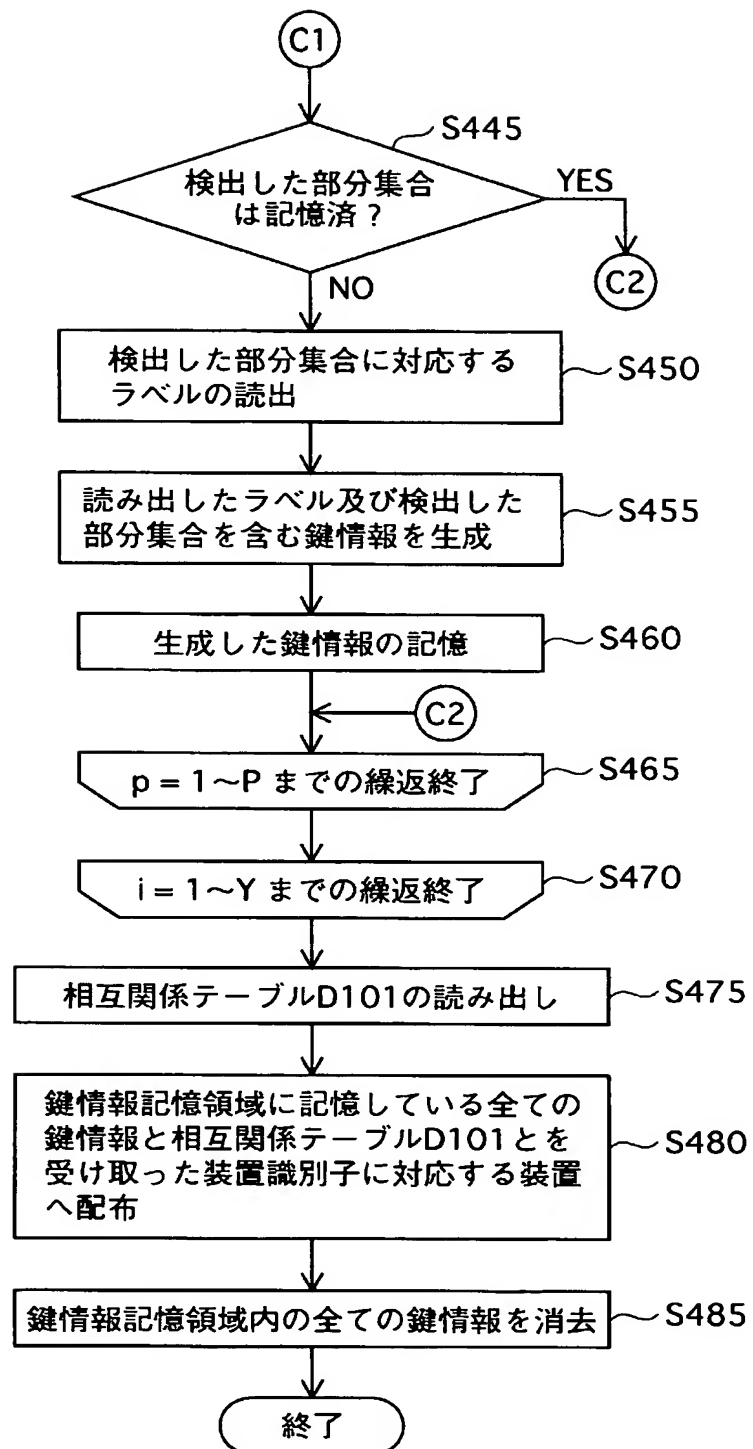
[図25]



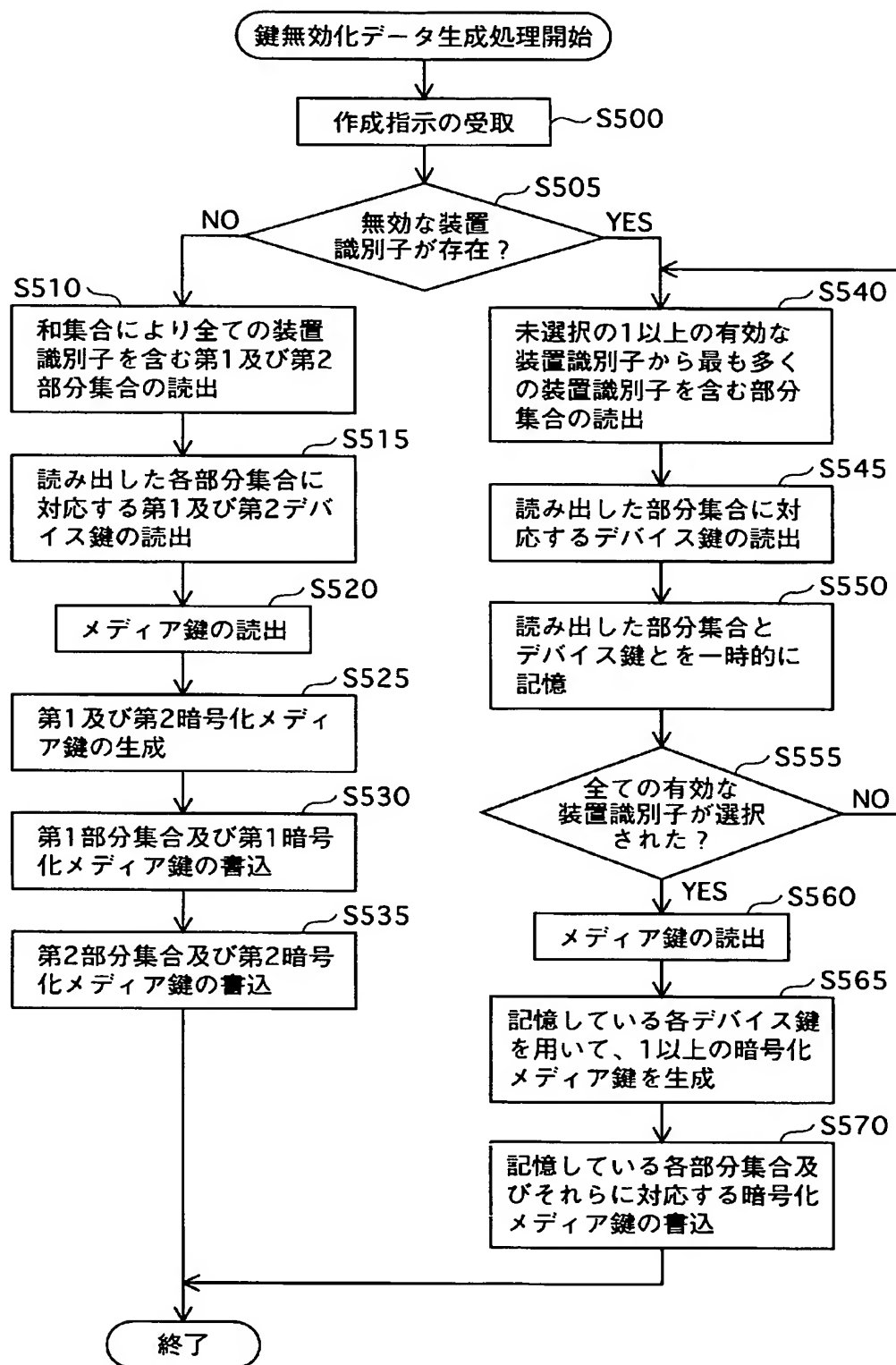
[図26]



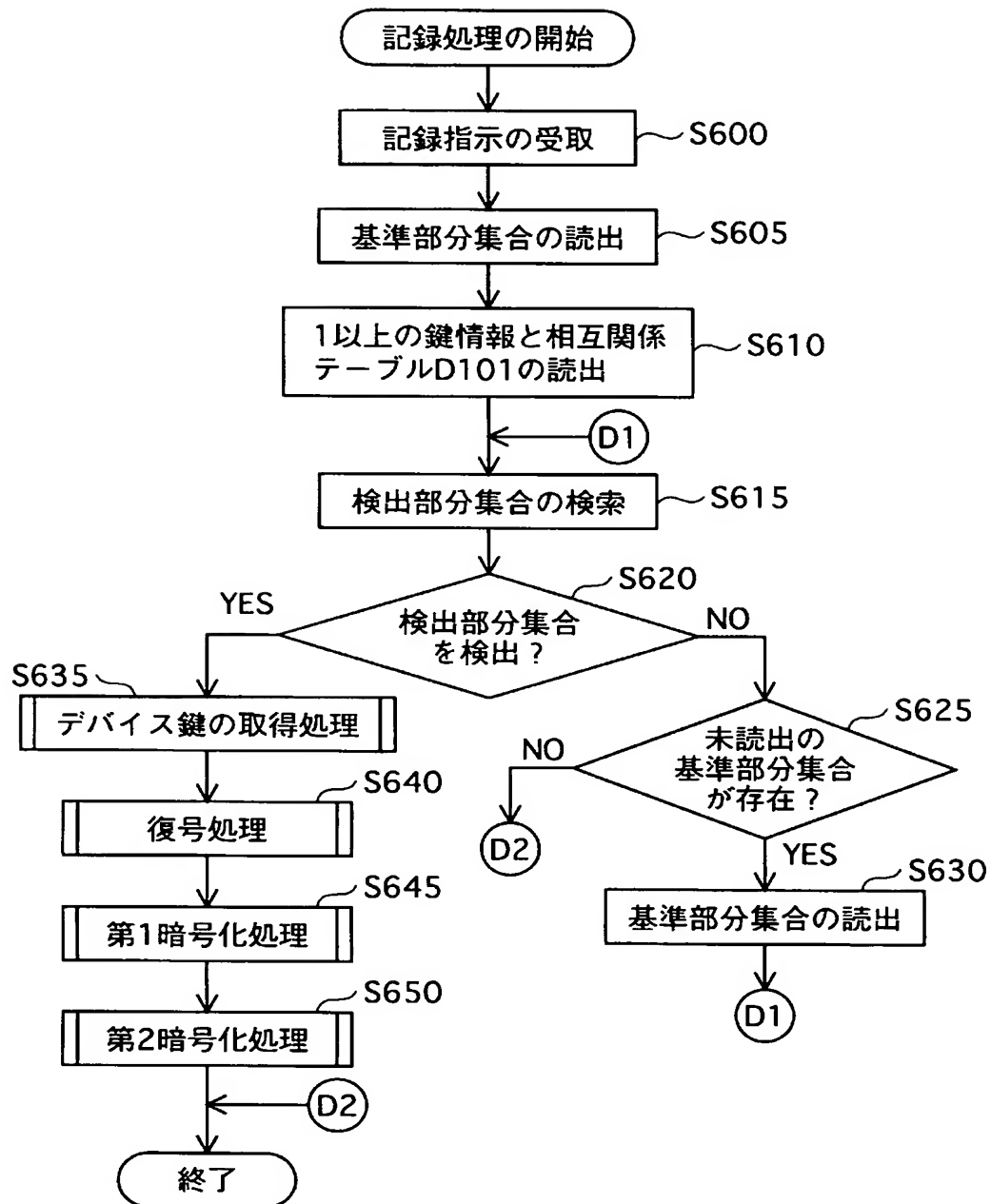
[図27]



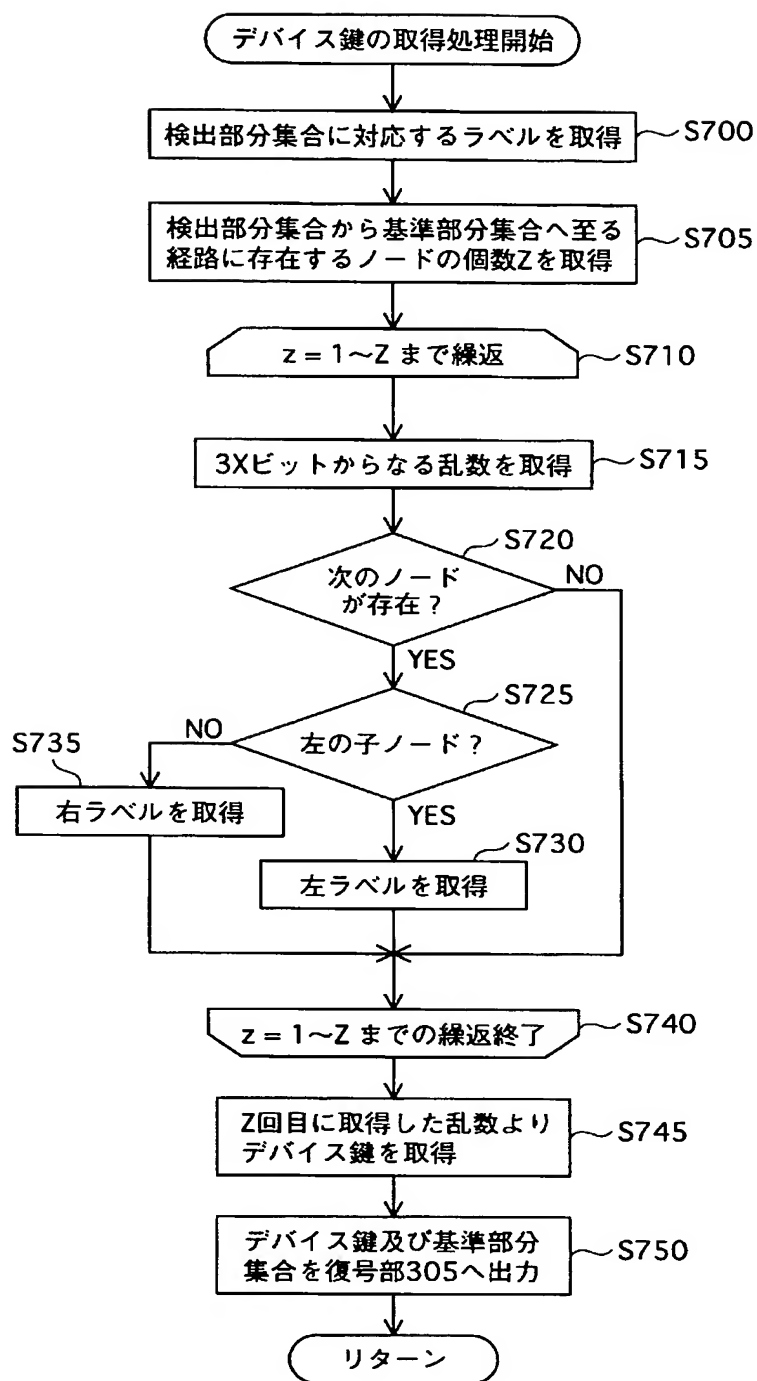
[図28]



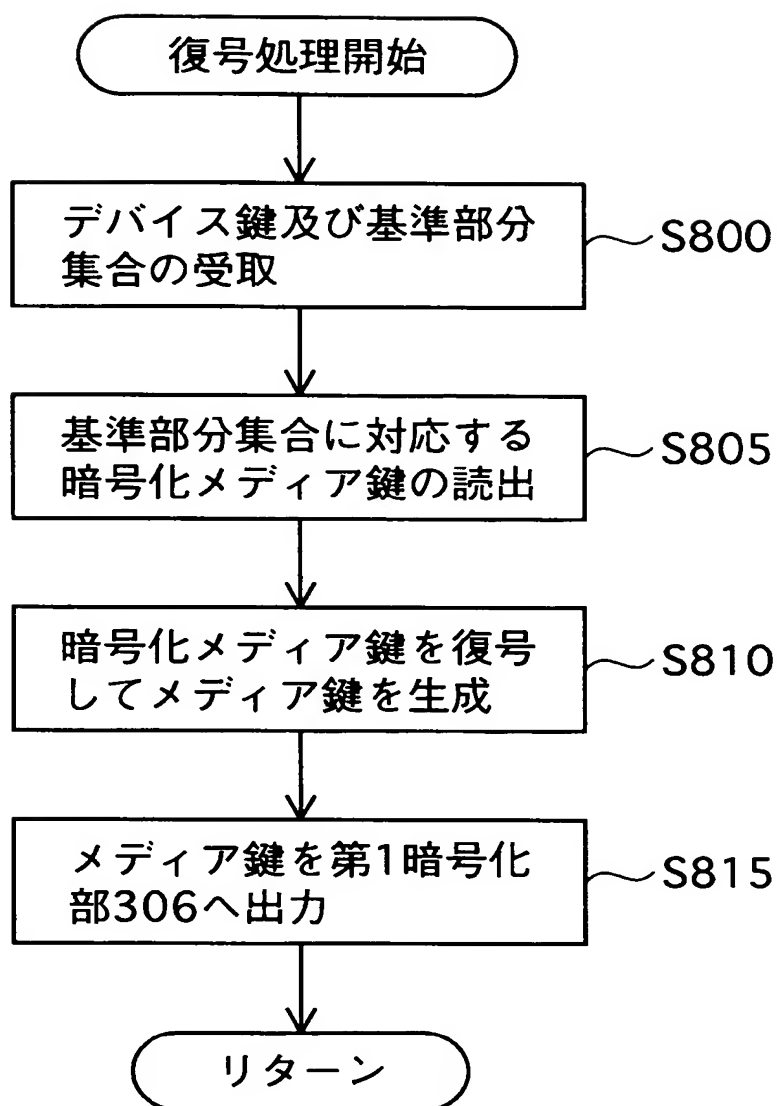
[図29]



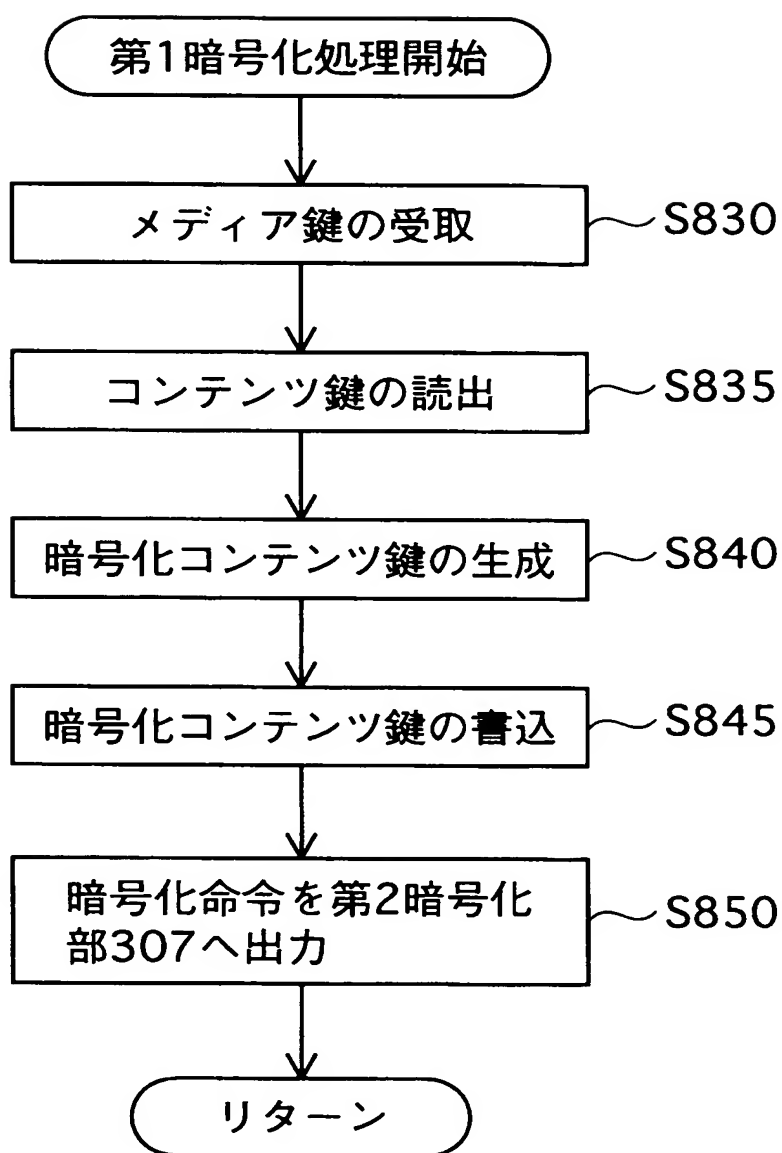
[図30]



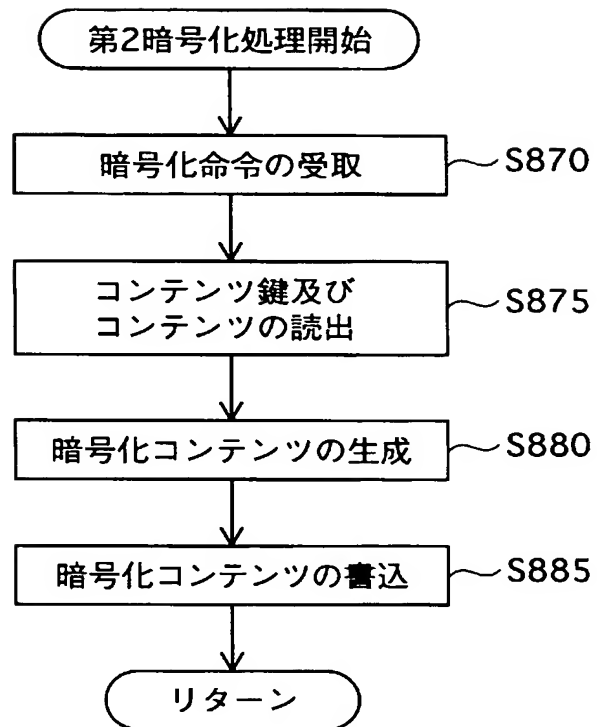
[図31]



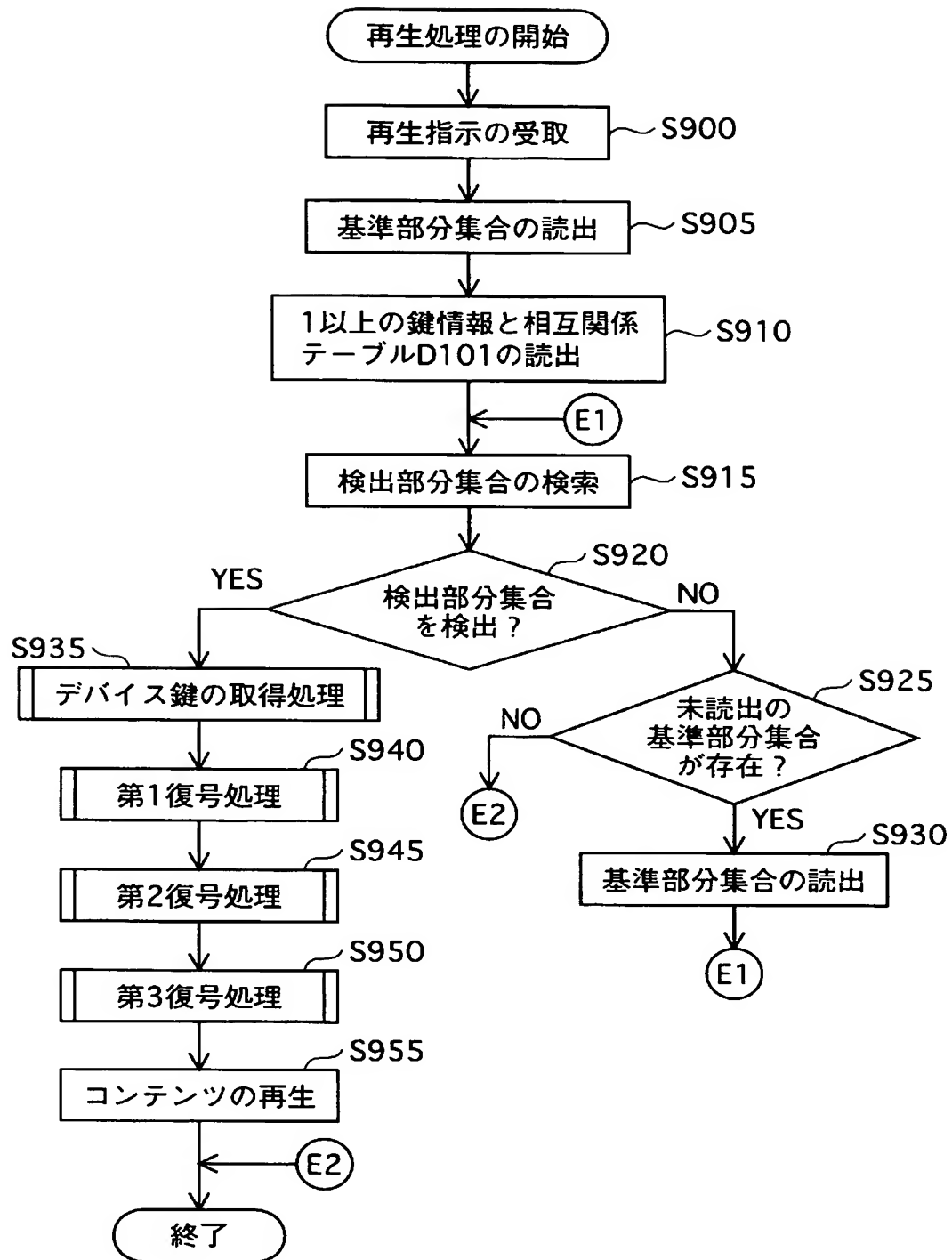
[図32]



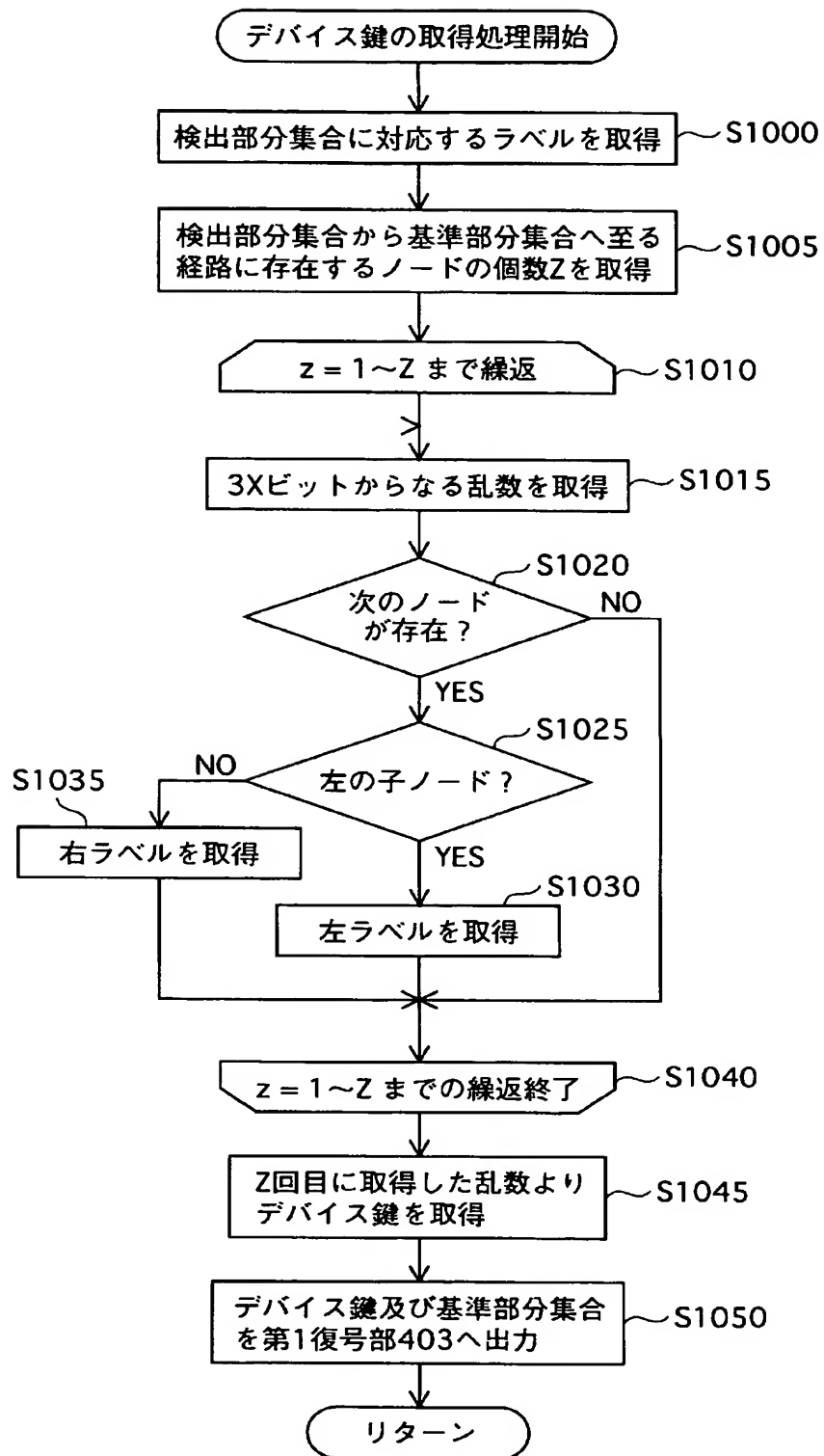
[図33]



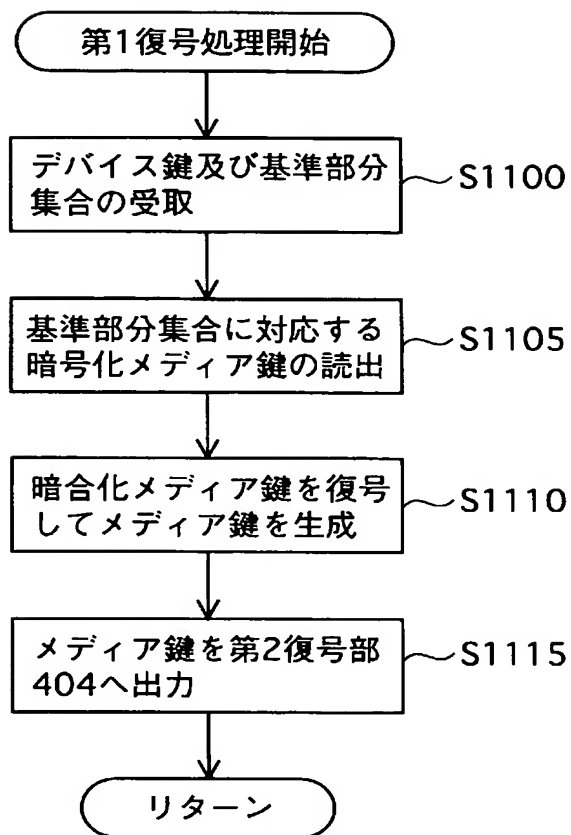
[図34]



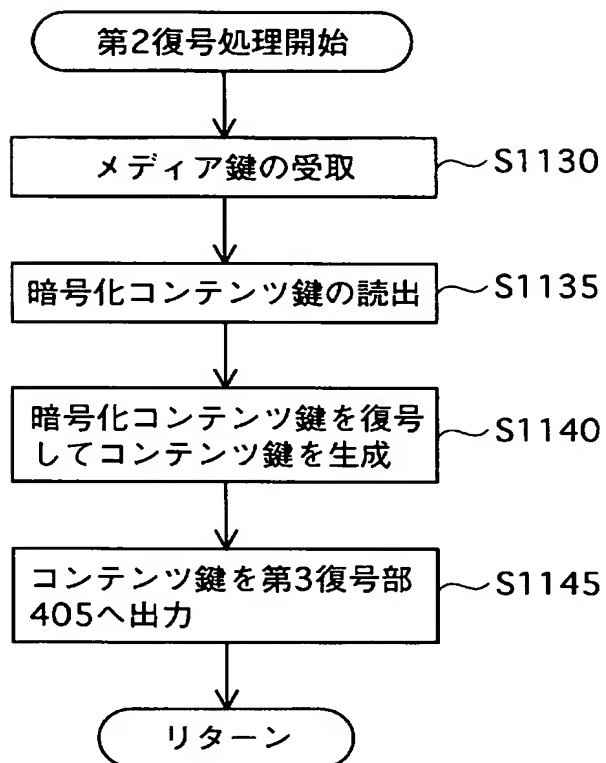
[図35]



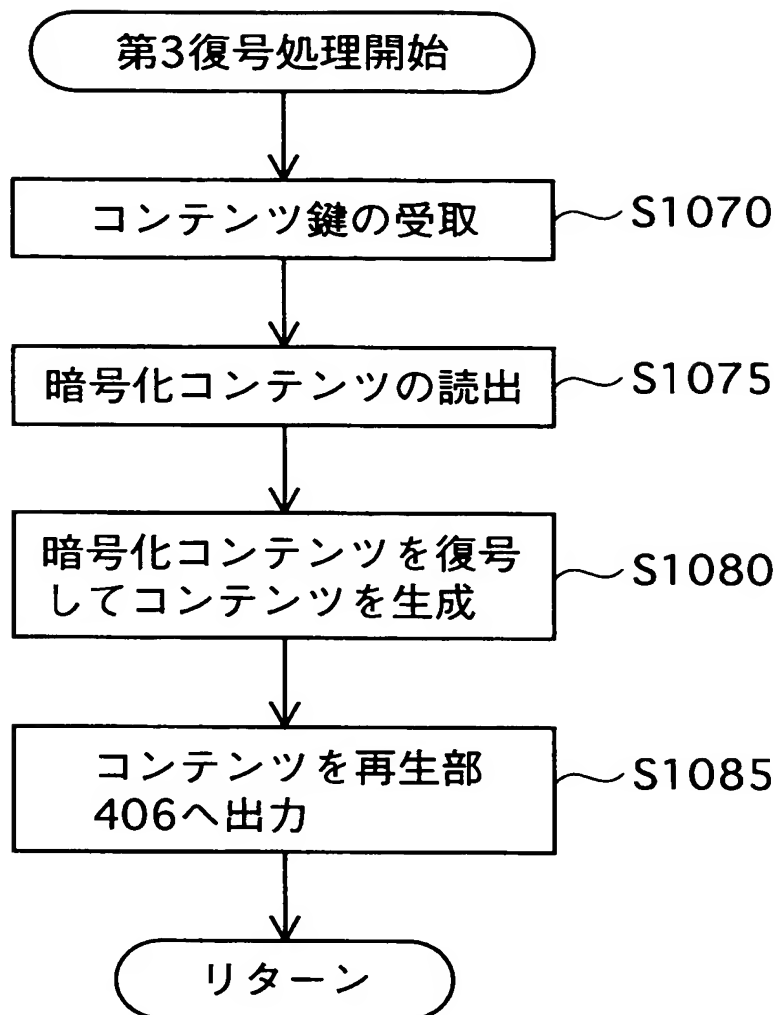
[図36]



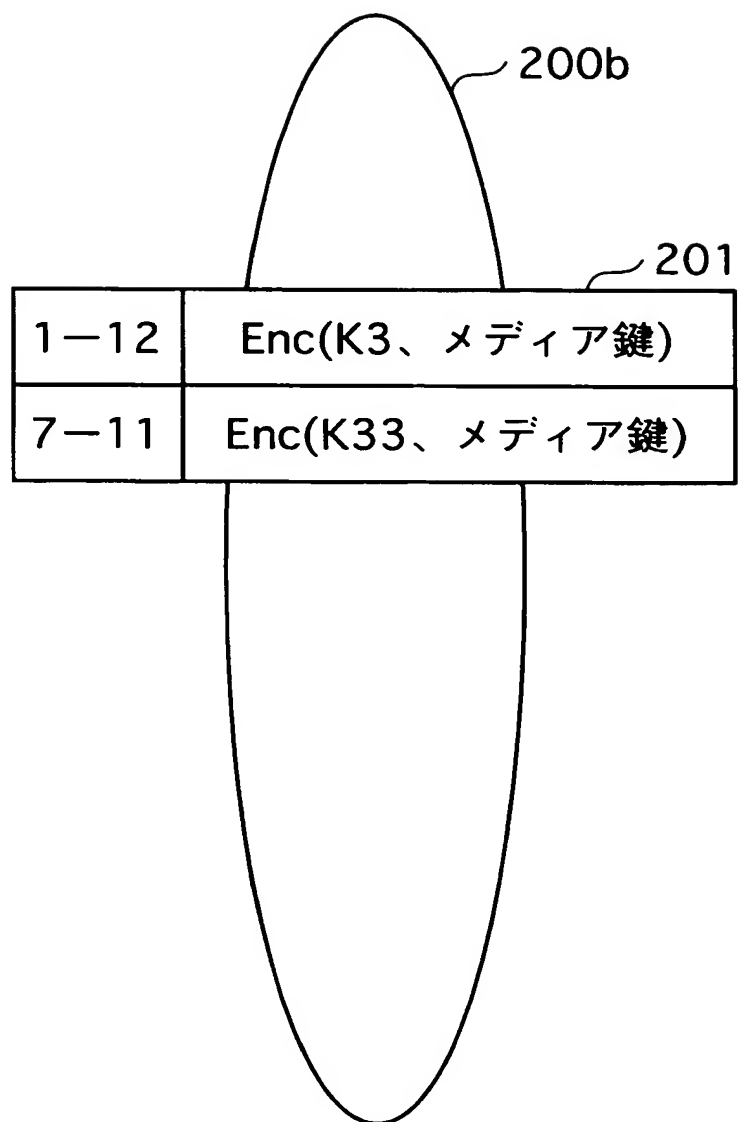
[図37]



[図38]



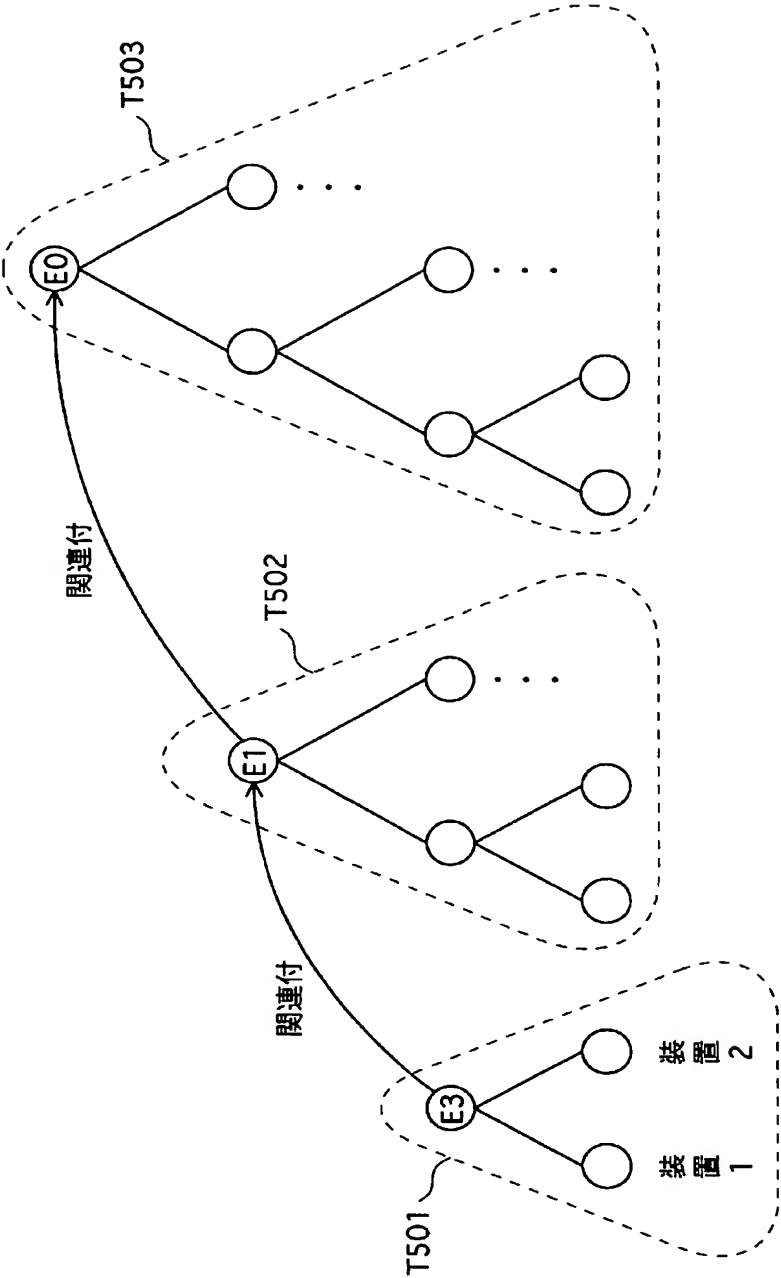
[図39]



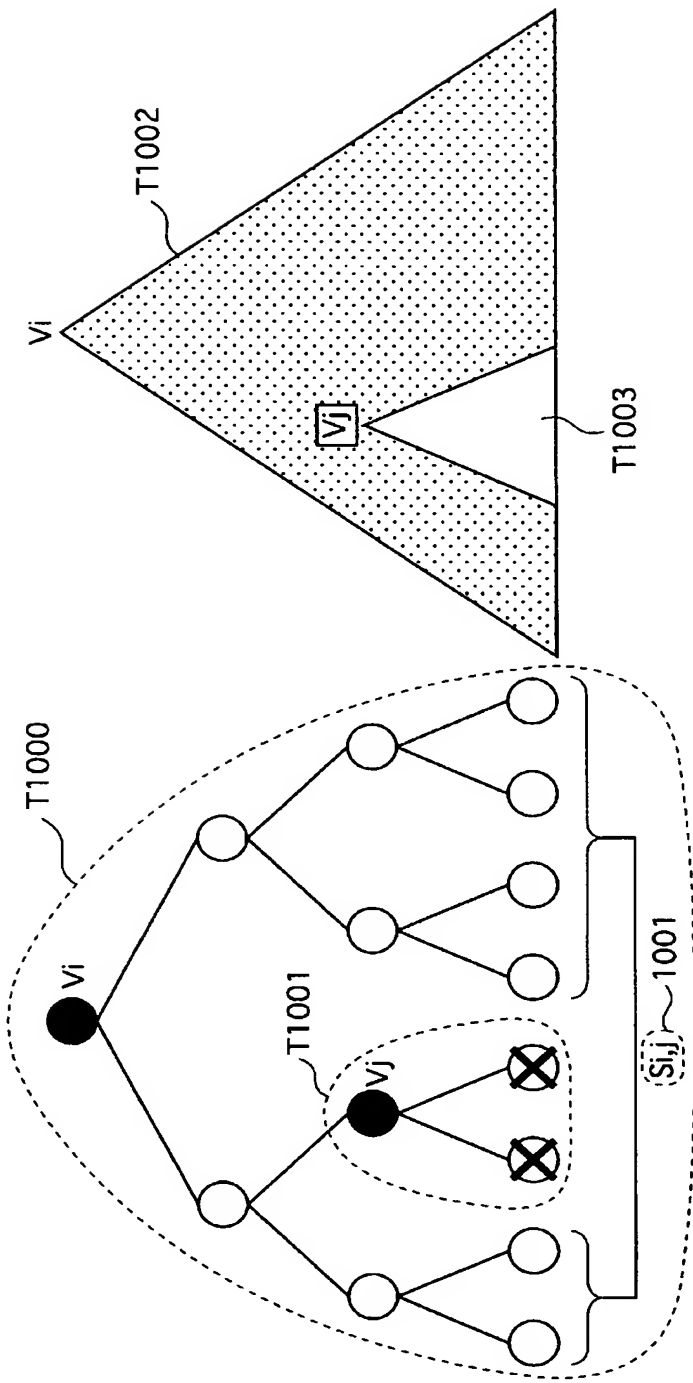
[図40]

装置名	合計	装置が保持する鍵情報							
		1-0 A1	3-12 A3RL	5-1212 A5RLRL	5-12112 A5RLRRL	5-12111 A5RLRRR			
装置1	4個 (-2)								
装置2	5個 (-1)	2-0 A2	1-1 A1R	3-11 A3RR	5-1212 A5RLRL	5-12111 A5RLRRR			
装置3	4個 (-2)	3-0 A3	1-12 A1RL	5-1211 A5RLRR	5-12122 A5RLRLL				
装置4	6個 (0)	4-0 A4	3-1 A3R	1-11 A1RR	1-121 A1RLR	5-1211 A5RLRR	5-12121 A5RLRLR		
装置5	4個 (-2)	5-0 A5	7-12 A7RL	1-1212 A1RLRL	1-12112 A1RLRRL				
装置6	5個 (-1)	6-0 A6	5-1 A5R	7-11 A7RR	1-1212 A1RLRL	1-12111 A1RLRRR			
装置7	4個 (-2)	7-0 A7	5-12 A5RL	1-1211 A1RLRR	1-12122 A1RLRLL				
装置8	6個 (0)	8-0 A8	7-1 A7R	5-11 A5RR	5-121 A5RLR	1-1211 A1RLRR	1-12121 A1RLRLR		

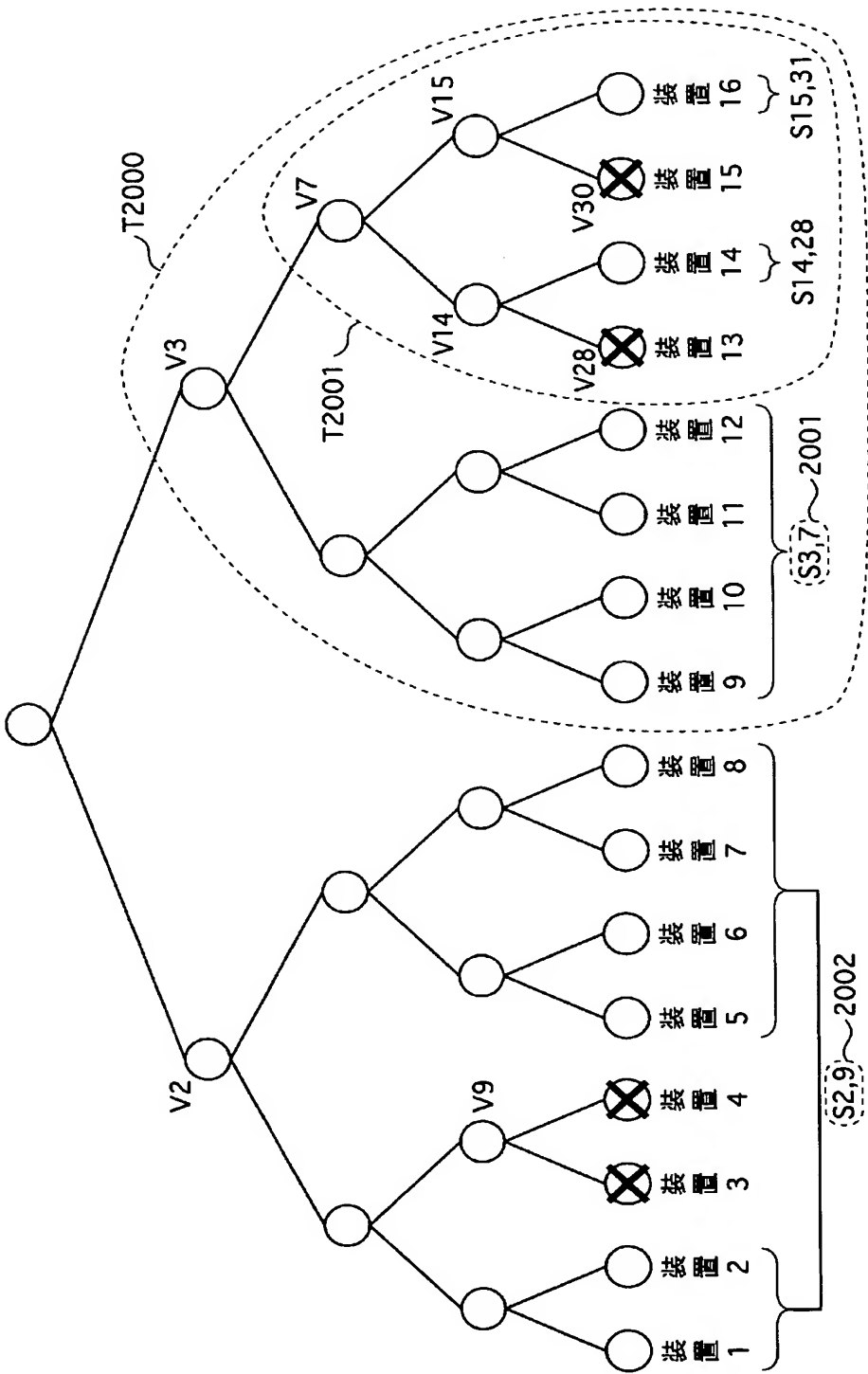
[図41]



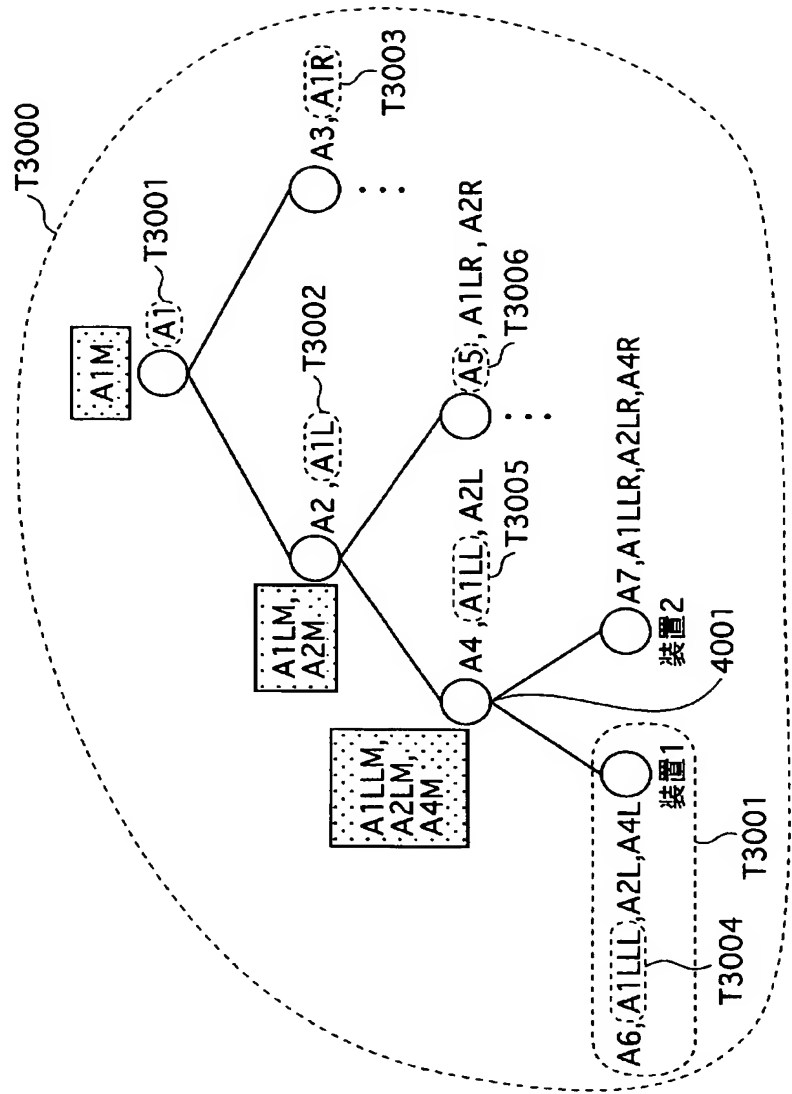
[図42]



[図43]



[図44]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2004/017453

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl⁷ H04L9/08

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl⁷ H04L9/08

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1922-1996 Toroku Jitsuyo Shinan Koho 1994-2005
Kokai Jitsuyo Shinan Koho 1971-2005 Jitsuyo Shinan Toroku Koho 1996-2005

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A X	D. Naor, M. Naor and J. Lotspiech, 'Revocation and Tracing Schemes for Stateless Receivers', Proceedings of CRYPTO2001, LNCS2139, pages 41 to 62, 2001.	1-36 39-42
A	JP 63-298523 A (Ricoh Co., Ltd.), 06 December, 1988 (06.12.88), Page 2, upper left column, line 2 to upper right column, line 2; Fig. 2 (Family: none)	1-36
A	JP 2002-281013 A (Matsushita Electric Industrial Co., Ltd.), 27 September, 2002 (27.09.02), Par Nos. [0023] to [0030] & US 2002-76204 A & EP 1215844 A	1-36

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:	"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A" document defining the general state of the art which is not considered to be of particular relevance	"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E" earlier application or patent but published on or after the international filing date	"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&" document member of the same patent family
"O" document referring to an oral disclosure, use, exhibition or other means	
"P" document published prior to the international filing date but later than the priority date claimed	

Date of the actual completion of the international search
02 February, 2005 (02.02.05)

Date of mailing of the international search report
22 February, 2005 (22.02.05)

Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2004/017453

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	JP 10-283270 A (Fujitsu Ltd.), 23 October, 1998 (23.10.98), Par Nos. [0067] to [0069]; Fig. 4 (Family: none)	37, 38

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2004/017453

Box No. II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

The inventions of claims 1-36, 39-42 relate to the technique for arranging device identifies identifying a plurality of terminal devices to leaves of a tree structure and assigning unique information serving as a base of a decoding key for decoding the encrypted data, to each of the device identifiers. The inventions of claims 37, 38 relates to encryption and storage of a medium key by an encryption key generated by using unique information on the terminal device. Accordingly, these groups of inventions are not so linked as to form a single general inventive concept. Consequently, the inventions of claims 1-42 do not satisfy the requirement of unity of invention.

1. ☒ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.
2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.
3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

- ☐ The additional search fees were accompanied by the applicant's protest.
- ☒ No protest accompanied the payment of additional search fees.

A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int. Cl⁷ H04L9/08

B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int. Cl⁷ H04L9/08

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1922-1996年
日本国公開実用新案公報	1971-2005年
日本国登録実用新案公報	1994-2005年
日本国実用新案登録公報	1996-2005年

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
A X	D. Naor, M. Naor, and J. Lotspiech, 'Revocation and Tracing Schemes for Stateless Receivers', Proceedings of CRYPTO2001, LNCS 2139, pages 41-62, 2001.	1-36 39-42
A	J P 63-298523 A (株式会社リコー) 1988. 12. 06, 第2頁左上欄第2行-右上欄第2行, 第2図 (ファミリ-なし)	1-36

☒ C欄の続きにも文献が列挙されている。☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」 特に関連のある文献ではなく、一般的技術水準を示すもの
「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)
「O」 口頭による開示、使用、展示等に言及する文献
「P」 国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「&」 同一パテントファミリー文献

国際調査を完了した日

02. 02. 2005

国際調査報告の発送日

22. 2. 2005

国際調査機関の名称及びあて先

日本国特許庁 (ISA/J P)

郵便番号100-8915

東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

青木 重徳

5M

3574

電話番号 03-3581-1101 内線 3597

C (続き) . 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
A	J P 2002-281013 A (松下電器産業株式会社) 2002.09.27, 段落【0023】-【0030】 & US 2002-76204 A & EP 1215844 A	1-36
X	J P 10-283270 A (富士通株式会社) 1998.10.23, 段落【0067】-【0069】, 図4 (ファミリーなし)	37, 38

第II欄 請求の範囲の一部の調査ができないときの意見 (第1ページの2の続き)

法第8条第3項(PCT17条(2)(a))の規定により、この国際調査報告は次の理由により請求の範囲の一部について作成しなかった。

1. ☐ 請求の範囲 _____ は、この国際調査機関が調査をすることを要しない対象に係るものである。つまり、
2. ☐ 請求の範囲 _____ は、有意義な国際調査をすることができる程度まで所定の要件を満たしていない国際出願の部分に係るものである。つまり、
3. ☐ 請求の範囲 _____ は、従属請求の範囲であってPCT規則6.4(a)の第2文及び第3文の規定に従って記載されていない。

第III欄 発明の単一性が欠如しているときの意見 (第1ページの3の続き)

次に述べるようにこの国際出願に二以上の発明があるときの国際調査機関は認めた。

請求の範囲1-36, 39-42に係る発明は、複数の端末装置を識別する各装置識別子を木構造のリーフに配し、各装置識別子に、暗号化されたデータを復号する復号鍵の基となる固有情報を割り当てる技術であって、第1及び第2の割り当て手段を有する技術であるのに対し、請求の範囲37, 38に係る発明は、端末装置の固有情報を用いて生成した暗号鍵によりメディア鍵を暗号化して記憶することを記載しており、単一の一般的発明概念を形成するように連関しているものではないので、請求の範囲1-42に係る発明は発明の単一性の要件を満たしていない。

1. ☒ 出願人が必要な追加調査手数料をすべて期間内に納付したので、この国際調査報告は、すべての調査可能な請求の範囲について作成した。
2. ☐ 追加調査手数料を要求するまでもなく、すべての調査可能な請求の範囲について調査することができたので、追加調査手数料の納付を求めなかった。
3. ☐ 出願人が必要な追加調査手数料を一部のみしか期間内に納付しなかったため、この国際調査報告は、手数料の納付のあった次の請求の範囲のみについて作成した。
4. ☐ 出願人が必要な追加調査手数料を期間内に納付しなかったため、この国際調査報告は、請求の範囲の最初に記載されている発明に係る次の請求の範囲について作成した。

追加調査手数料の異議の申立てに関する注意

- ☐ 追加調査手数料の納付と共に出願人から異議申立てがあった。
☒ 追加調査手数料の納付と共に出願人から異議申立てがなかった。